CONSEJO DENTISTAS
ORGANIZACIÓN COLEGIAL DE DENTISTAS DE ESPAÑA

# LA NORMATIVA DE PROTECCIÓN DE DATOS (RGPD-GDPR)

**Guía práctica para Odontólogos y Estomatólogos sobre el impacto del Reglamento Europeo de Protección de Datos.**

# ÍNDICE

## NECESIDAD DE REGULAR LOS TRATAMIENTOS DE DATOS. EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

El pasado 4 de mayo de 2016, se publicó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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, por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD), entrando en vigor a los 20 días de su publicación y cuya aplicación obligatoria y directa a todos los Estados miembros de la Unión Europea será a partir del 25 de mayo de 2018.

La aprobación de este Reglamento pone fin a más de cuatro años de trabajo, dado que el primer proyecto presentado por parte de la Comisión Europea data de 25 de enero de 2012. Las tecnologías de la información y comunicación han sufrido tal progreso y perfeccionamiento, que la tendencia hoy en día es el uso de las herramientas digitales frente al manejo de documentación física.

Esta realidad trasciende la esfera profesional y son numerosas organizaciones las que invierten su economía en implantar sistemas de gestión de la información, suponiendo con ello un aumento en su volumen de negocio gracias al tratamiento automatizado de importantes cantidades de bases de datos que serían imposibles de procesar con cualquier otro método.

En sentido contrario, los ciudadanos han perdido el control sobre sus datos. Desconocen el uso que le dan las organizaciones a sus datos personales, muchas veces por dejadez a saberse informados, otras muchas porque los responsables ocultan los verdaderos fines de obtención mediante cláusulas extremadamente genéricas y en la mayoría de los casos, porque el desarrollo tecnológico dificulta la comprensión de la vida útil del dato, esto es, como se

obtiene, como se procesa, como se conserva y como se devuelve y/o destruye.

Ante este suceso, la única defensa jurídica que existía era la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos y su normativa de transposición, que en España es la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), ambas de los años 90. Lógicamente poco amparo pueden recibir los ciudadanos y poca regulación pueden recibir soluciones tales como la computación en nube o *cloud computing,* con normativas que fueron aprobadas en una época donde apenas existía *internet*.

Otra realidad patente, es que aquella regulación se motivó sobre la base de una directiva que, como bien es sabido, posibilita a los Estados miembros a decidir sobre la forma y medios para conseguir los resultados pretendidos por ella. Consecuencia de esto, fue que cada país reguló la materia de protección de datos conforme a sus propios criterios y conveniencia.

Viviendo en un mundo donde los traspasos de información no conocen de delimitaciones geográficas, este modelo de directiva había quedado radicalmente obsoleto. La sociedad demandaba implantar un modelo de gobierno único armonizado, y aparentemente el RGPD será la solución para todos los Estados miembros de la Unión Europea.

## ¿CÓMO AFECTA EL RGPD A LOS ODONTÓLOGOS Y ESTOMATÓLOGOS?

Los odontólogos y estomatólogos colegiados en sus respectivos Colegios Oficiales, así como las clínicas y/o consultorios dentales, son a todos los efectos los "Responsables" de los tratamientos de datos de carácter personal, puesto que recopilan datos y deciden sobre la finalidad de su uso, por lo que deben adaptarse a estas nuevas exigencias marcadas desde la Unión Europea.

Además, dado que su finalidad principal de recogida de datos es la de prestar un servicio de asistencia sanitaria, los esfuerzos deberán ser mayores a la hora de aplicar medidas de seguridad sobre los datos personales de sus pacientes.

El ámbito sanitario se diferencia del resto en que, en el marco de los procesamientos de datos, los datos personales no íntimos casi siempre van asociados a datos íntimos de especial protección (la historia clínica). Cabe advertir, además, que, la actuación del profesional sanitario en relación con sus pacientes, y de la asistencia sanitaria que éste les presta, está basada en una relación de confianza que lleva intrínsecamente aparejada la salvaguarda de la intimidad, confidencialidad y respeto a la información proporcionada al profesional por parte del paciente.

Los odontólogos y estomatólogos, por sus propias funciones, tratan datos **sensibles** de sus pacientes, por ello, deben ser especialmente conscientes de la responsabilidad que implica su tratamiento y garantizar a sus pacientes que se vela por el cumplimiento de la normativa de protección de datos, para evitar, de este modo, eventuales fugas de información o accesos no autorizados a sus datos personales.

## ¿QUÉ SE ENTIENDE EN EL NUEVO REGLAMENTO POR DATO DE CARÁCTER PERSONAL?

En esta nueva regulación se sigue entendiendo por dato de carácter personal todos los datos que se pueden atribuir a una persona identificada o identificable (titular de sus datos).

Una persona puede llegar a identificarse cuando su identidad se puede concretar mediante una serie de elementos tales como por ejemplo un nombre, sus siglas, un número de identificación (nº de historia clínica), datos de localización o por ejemplo mediante el visionado de imágenes.

## OTRAS DEFINICIONES A TENER EN CUENTA

| |
|---|
| **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción; |
| **Elaboración de perfiles**: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física; |

| |
|---|
| **Seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable; |
| **Responsable del tratamiento o responsable**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; |
| **Encargado del tratamiento o encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento; |
| **Consentimiento del interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen; |

| |
|---|
| **Violación de la seguridad de los datos personales**: toda violación de la seguridad 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 autorizados a dichos datos; |
| **Autoridad de Control**: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51; En España, es la Agencia Española de Protección de Datos. |

## DEFINICIONES DE DATOS QUE REQUIEREN DE ESPECIAL PROTECCIÓN

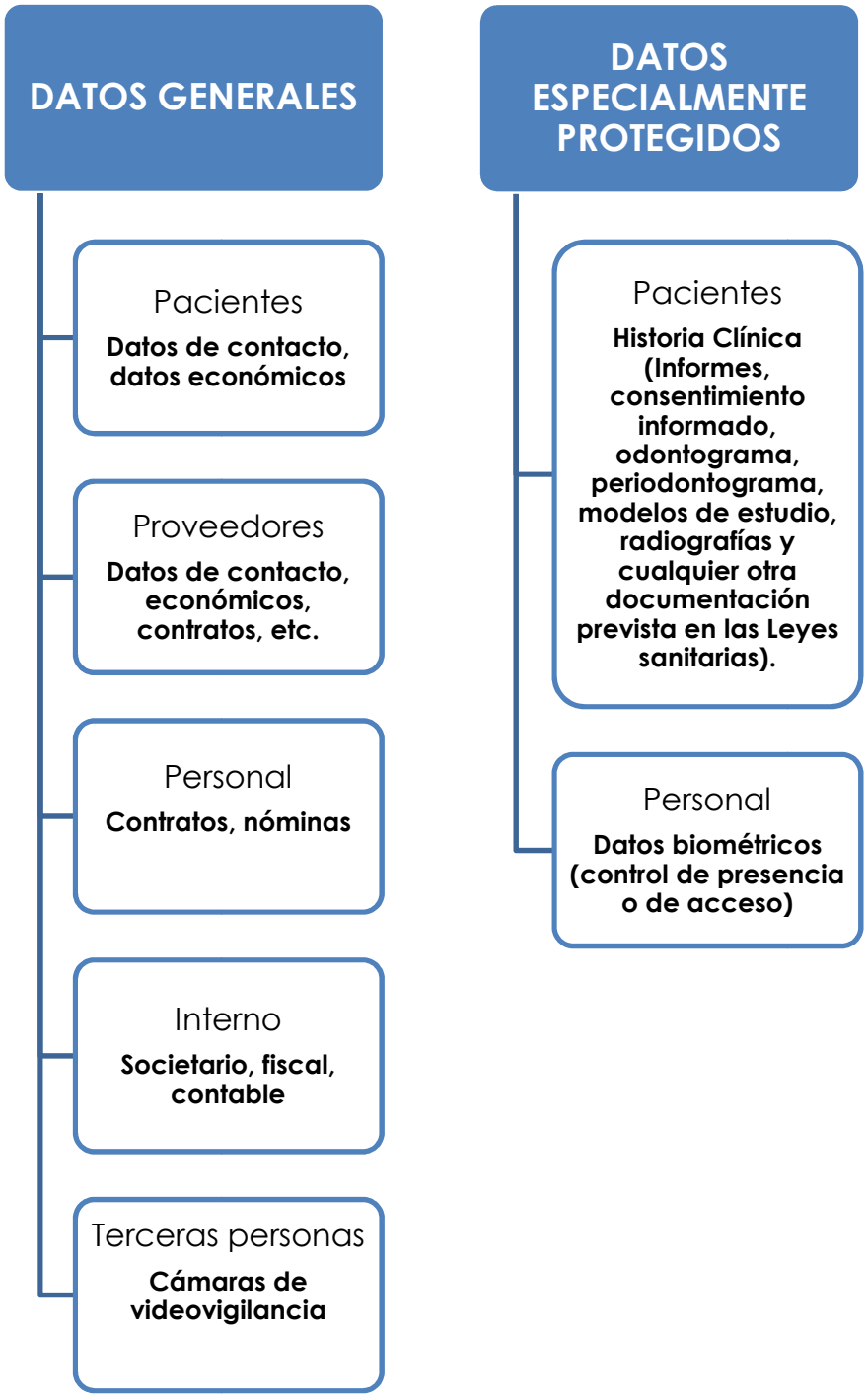
El RGPD ha ampliado y definido de forma más acertada este tipo de datos.
En el ámbito sanitario debemos tener en cuenta estas definiciones,

| |
|---|
| **Datos relativos a la salud**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud; |

| |
|---|
| **Datos genéticos**: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona; |
| **Datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos; |

En conclusión, es importante tener clara la tipología del dato, que podemos resumir en lo siguiente:

## ¿QUÉ DATOS SUELEN TRATAR LOS ODONTÓLOGOS Y ESTOMATÓLOGOS?



## NOVEDADES DEL RGPD. EL RIESGO

El RGPD pretende consolidar una verdadera cultura de privacidad para los responsables con el fin último de proteger de forma eficiente los datos personales de todos los ciudadanos europeos. Lo que hasta la fecha suponía una obligación legal de protección del dato personal pasa a convertirse en un nuevo modelo de privacidad.

La principal novedad de este RGPD es la puesta en funcionamiento de procedimientos de prevención del riesgo, con la incorporación de medidas correspondientes para identificar los riesgos derivados del tratamiento de datos, la valoración de la probabilidad de que ocurran, del daño que causarían si se materializasen y de las medidas a adoptar en caso de que efectivamente sucedan. Para ello el RGPD propone que los responsables del tratamiento actúen de conformidad con el principio de *accountability* o responsabilidad proactiva.

Este principio de *accountability* o responsabilidad proactiva obliga además al responsable a estar en condiciones de demostrar en todo momento que cumple con las previsiones normativas en materia de protección de datos (principio de rendición de cuentas).

**Los Responsables deben adoptar medidas para acreditar el correcto tratamiento y recogida de los datos personales de sus pacientes.**

Pues bien, para poder analizar correctamente los posibles riesgos el RGPD introduce como novedades los siguientes elementos:

## 1. ¿QUÉ INFORMACIÓN SE DEBE DAR A LOS PACIENTES PARA RECABAR SUS DATOS?

Se hace hincapié en la información que se le debe proporcionar a los interesados, la cual debe ser clara y comprensible, con unos clausulados más transparentes y detallados, diferenciando todas las distintas finalidades del tratamiento. Se deberá informar sobre:

- ✓ La identidad y los datos de contacto del **responsable** y del **delegado de protección de datos,** si cabe.
- ✓ Los **derechos** de los interesados.
- ✓ El derecho del interesado a **retirar su consentimiento**.
- ✓ Los **fines** y la **base jurídica** del tratamiento de los datos.
- ✓ El **interés legítimo del responsable**.
- ✓ Los **destinatarios** de los datos personales.
- ✓ El derecho a presentar una **reclamación.**
- ✓ **Requisito legal o contractual** que obliga a la comunicación de datos, y las consecuencias de no facilitar los datos pedidos.
- ✓ Si se va a proyectar un **fin ulterior** distinto del fin inicial, se informará antes del nuevo tratamiento.
- ✓ La **transferencia** de datos a un **tercer país o** a una **organización internacional**.
- ✓ El **plazo de conservación** de los datos personales.
- ✓ **Decisiones automatizadas**, como la elaboración de perfiles.

**Los Responsables deben cumplir con esta obligación de información con la utilización de nuevas cláusulas y utilización de forma complementaria de carteles informativos.**

## 2. ¿ESPECIAL REFERENCIA A LOS PLAZOS DE CONSERVACIÓN DE DATOS PERSONALES?

Cobra especial importancia informar al interesado sobre los plazos de conservación de los datos personales ya que en virtud del RGPD los datos obtenidos serán adecuados, pertinentes y limitados a lo necesario, en relación con los fines para los que son tratados.

Por lo tanto, entre otras, deberá tenerse en cuenta los plazos establecidos en la normativa específica sanitaria en relación con la conservación de la Historia Clínica.

| | **HISTORIA CLÍNICA** | |
|---|---|---|
| **PLAZO** | **DOCUMENTOS** | **REF. LEGAL** |
| **Mín. 5 AÑOS** | Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial | Artículo 17.1 de la **Ley 41/2002** de 14 noviembre, de autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica |
| **OTROS SUPUESTOS** | La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas. | Artículo 17.2 de la Ley 41/2002 de 14 noviembre, de autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica |
| **5 AÑOS** | Para garantizar los usos futuros de la historia clínica, especialmente el asistencial, se conservará el tiempo mínimo establecido en la normativa básica estatal, contado desde la fecha del alta de cada proceso asistencial o desde el fallecimiento del paciente. | Ley 10/2014, de 29 diciembre, de la CA **Valenciana** (Salud) |
| **5 AÑOS / INDEFINIDO** | La historia clínica habrá de conservarse en | Artículo 20 de la Ley 3/2001, |

| | | |
|---|---|---|
| | condiciones que garanticen la preservación de la información asistencial que contiene, aunque no se mantenga en el soporte original en el cual se ha generado, con las cautelas que se establezcan reglamentariamente para evitar la manipulación de datos cuando no se mantenga dicho soporte original.2.- Se conservará indefinidamente la siguiente información:<br><br>- Informes de alta.<br>– Hojas de consentimiento informado.<br>– Hojas de alta voluntaria.<br>– Informes quirúrgicos y/o registros de parto.<br>– Informes de anestesia.<br>– Informes de exploraciones complementarias.<br>– Informes de necropsia.<br>– Hoja de evolución y de planificación de cuidados de enfermería.<br>– Otros informes médicos.<br>– Cualquier otra información que se considere relevante a efectos asistenciales, preventivos, epidemiológicos o de investigación.<br>– La información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales.<br><br>El resto de la información se conservará, como mínimo, hasta que transcurran cinco años desde la última asistencia prestada al paciente o desde su fallecimiento. | de 28 mayo CA **Galicia**, consentimiento informado e historia clínica de los pacientes |
| **15 AÑOS** | La historia clínica se ha de conservar como mínimo hasta quince años desde la muerte del paciente. No obstante, se podrán seleccionar y destruir los documentos que no sean relevantes para la asistencia, transcurridos dos años desde la última atención al paciente.<br><br>En todo caso, en la historia clínica se han de conservar durante quince años como mínimo contados desde la muerte del paciente, y junto con los datos de identificación del paciente: las hojas de consentimiento informado, los informes de alta, los informes quirúrgicos y el registro de parto, los datos relativos a la anestesia, los informes de exploraciones complementarias y los informes de necropsia.<br><br>Sin perjuicio de lo establecido en los apartados 1 y 2 de este artículo, la documentación que a criterio del facultativo sea relevante a efectos preventivos, asistenciales o epidemiológicos se conservará el tiempo que se considere oportuno. | Artículo 72 Ley 7/2002 de 10 diciembre CA **Cantabria**, ordenación sanitaria. |
| **5 AÑOS** | Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial. | Artículo 61 de la Ley Foral 17/2010, de 8 noviembre, **Navarra**, de los derechos y deberes de las personas en materia de salud |

| | | |
|---|---|---|
| | En cualquier caso, en la historia clínica deben conservarse, junto con los datos de identificación del paciente, durante cinco años, como mínimo, a contar desde la muerte del paciente: las hojas de consentimiento informado, los informes de alta, los informes quirúrgicos y el registro de parto, los datos relativos a la anestesia, los informes de exploraciones complementarias y los informes de necropsia.<br><br>La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas. | |
| **15 AÑOS** | De la historia clínica debe conservarse, junto con los datos de identificación de cada paciente, como mínimo durante quince años desde la fecha de alta de cada proceso asistencial, la siguiente documentación:<br>a) Las hojas de consentimiento informado.<br>b) Los informes de alta.<br>c) Los informes quirúrgicos y el registro de parto.<br>d) Los datos relativos a la anestesia.<br>e) Los informes de exploraciones complementarias.<br>f) Los informes de necropsia.<br>g) Los informes de anatomía patológica.<br>5. Los procesos de digitalización de la historia clínica que se lleven a cabo deben facilitar el acceso a la historia clínica desde cualquier punto del Sistema Nacional de Salud. A tal efecto, deben establecerse los mecanismos para hacer posible, mediante la tarjeta sanitaria individual, la vinculación entre las historias clínicas que cada paciente tenga en los organismos, centros y servicios del Sistema Nacional de Salud, y que permitan el acceso de los profesionales sanitarios a la información clínica y el intercambio de dicha información entre los dispositivos asistenciales de las comunidades autónomas, de conformidad con las disposiciones sobre protección de datos de carácter personal.<br>La documentación que integra la historia clínica no mencionada por el apartado 4 puede destruirse una vez hayan transcurrido cinco años desde la fecha de alta de cada proceso asistencial.<br>No obstante lo establecido por los apartados 4 y 6, debe conservarse de acuerdo con los criterios que establezca la comisión técnica en materia de documentación clínica, a la que hace referencia la disposición final primera, la documentación que sea relevante a efectos asistenciales, que debe incorporar el documento de voluntades anticipadas, y la documentación que sea relevante, especialmente, a efectos epidemiológicos, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. En el tratamiento de esta documentación debe evitarse identificar a las | L 21/2000 de 29 Dic. CA **Cataluña** (derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica) |

| | | |
|---|---|---|
| | personas afectadas, salvo que el anonimato sea incompatible con las finalidades perseguidas o que los pacientes hayan dado su consentimiento previo, de acuerdo con la normativa vigente en materia de protección de datos de carácter personal. La documentación clínica también debe conservarse a efectos judiciales, de conformidad con la normativa vigente.<br>La decisión de conservar la historia clínica, en los términos establecidos por el apartado 7, corresponde a la dirección médica del centro sanitario, a propuesta del facultativo o facultativa, previo informe de la unidad encargada de la gestión de la historia clínica en cada centro. Esta decisión corresponde a los propios facultativos cuando desarrollen su actividad de forma individual.<br>Los responsables de custodiar la historia clínica, a quienes se refiere el apartado 1, también son responsables de destruir correctamente la documentación que previamente se haya decidido expurgar.<br>En el supuesto de cierre de centros y servicios sanitarios, o de cese definitivo de actividades profesionales sanitarias a título individual, debe garantizarse el mantenimiento del acceso legalmente reconocido a las historias clínicas que se encuentren bajo la custodia de dichos centros o profesionales, en beneficio de la asistencia médica y, especialmente, de los derechos de los pacientes en materia de documentación clínica y de protección de datos personales.<br>Son aplicables a la conservación de la historia clínica, al proceso de traslación de información establecido por el apartado 3 y a la actividad de destrucción a la que se refiere el apartado 9 las medidas técnicas y organizativas de seguridad aplicables a los ficheros que contienen datos de carácter personal, en los términos establecidos por la normativa reguladora de la protección de datos de carácter personal.<br>1Las prescripciones del presente artículo se entienden sin perjuicio de la aplicación de la normativa específica de prevención de riesgos laborales y de protección de la salud de los trabajadores en las historias clínicas relativas a la vigilancia de la salud de los trabajadores. | |
| | La conservación de la historia clínica se rige por lo dispuesto en la legislación básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, teniendo los centros sanitarios la obligación de conservar las historias clínicas en condiciones que garanticen su seguridad y correcta conservación, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial. | Artículo 29.2 D 178/2005 de 26 Jul. CA **Canarias** Regl. que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos |

| | | |
|---|---|---|
| **5 AÑOS** | **A)** Podrán ser destruidos a partir de los cinco años desde la fecha de alta de cada episodio asistencial, los siguientes documentos contenidos en su historia clínica:<br>**a)** Hoja clínico-estadística.<br>**b)** Hoja del recién nacido, en la historia clínica de la madre.<br>**c)** Hoja de solicitud de interconsulta y pruebas complementarias, siempre que no contenga el resultado de la prueba complementaria.<br>**d)** Hoja de controles y cuidados específicos de enfermería.<br>**e)** Gráficas de constantes.<br>**f)** Hoja de urgencias.<br>**g)** Radiografías y otros documentos iconográficos, conservando los informes.<br>**B)** Igualmente podrán destruirse a partir de los cinco años, las hojas de anamnesis y de exploración física y las hojas de evolución de los episodios asistenciales de los que exista informe de alta. | |
| **20 AÑOS** | Transcurridos veinte años desde la última actividad asistencial recogida en la historia clínica, podrán ser destruidos los siguientes documentos:<br><br>**a)** Hoja de Autorización de ingreso.<br>**b)** Hoja de consentimiento informado.<br>**c)** Hoja quirúrgica.<br>**d)** Hoja de órdenes médicas.<br>**e)** Hoja de control de medicación.<br>**f)** Hoja de parto.<br>**g)** Hoja del recién nacido, de su propia historia clínica.<br>**h)** Hoja de anestesia.<br>**i)** Hoja de transfusión.<br>**j)** Informes de exploraciones complementarias.<br>**k)** Hoja de alta voluntaria.<br>**l)** Informes de Anatomía Patológica.<br>**m)** Informes de necropsias.<br>**n)** Otros documentos que no aparezcan citados en el presente artículo. | Artículo 29.3 D 178/2005 de 26 Jul. CA **Canarias** Regl. que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos |
| **SIEMPRE** | Se conservarán de manera definitiva:<br><br>**A)** Los informes clínicos de alta.<br>**B)** Las hojas de anamnesis y exploración física y las hojas de evolución de los episodios asistenciales de los que no exista informe de Alta. | Artículo 29.4 D 178/2005 de 26 Jul. CA **Canarias** Regl. que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos. |
| **5 AÑOS** | La documentación clínica generada deberá conservarse durante un periodo mínimo de cinco años a contar desde la fecha del alta de cada episodio asistencial | Art. 19.1 del Decreto 38/2012, de 13 de marzo, **País Vasco**, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica |
| **OTROS PLAZOS** | En aquellos casos en que exista normativa específica que establezca períodos de | Art. 19. 2 del Decreto 38/2012, de 13 de marzo, **País Vasco**, |

| | | |
|---|---|---|
| | conservación superiores a los establecidos en este Decreto la persona titular del centro sanitario correspondiente garantizará su cumplimiento. Específicamente deberá mantener la documentación clínica generada en los servicios de medicina nuclear y radioterapia durante el periodo de treinta años que se prevé en elReal Decreto 1841/1997, de 5 de diciembre (LA LEY 4327/1997), por el que se establecen los criterios de calidad en medicina nuclear, y en elReal Decreto 1566/1998, de 17 de julio (LA LEY 3328/1998), por el que se establecen los criterios de calidad en radioterapia, respectivamente. | sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica |
| **EXPURGO Y DESTRUCCIÓN** | Una vez transcurridos los plazos legales de conservación a que se refiere o que determina este Decreto, se podrá realizar un proceso de expurgo de la documentación clínica, pudiéndose destruir los tipos documentales que procedan con excepción de los siguientes:<br><br>**a)** Informe de alta.<br>**b)** Informe clínico de consultas externas.<br>**c)** Informe clínico de urgencias.<br>**d)** Informe clínico de atención primaria.<br>**e)** Informe de resultados de pruebas de laboratorio, modelo B.<br>**f)** Informe de pruebas de imagen.<br>**g)** Informe de cuidados de enfermería.<br>**h)** Consentimiento informado.<br>**i)** Hojas de alta voluntaria.<br>**j)** Informe quirúrgico.<br>**k)** Informe de parto.<br>**l)** Informe de anestesia.<br>**m)** Informe de exploraciones complementarias.<br>**n)** Informe de anatomía patológica.<br>Una vez transcurridos 10 años tras el fallecimiento de la persona paciente, se podrá destruir toda su documentación clínica, de acuerdo con lo que se establece en este Decreto.<br>Se podrá destruir asimismo la historia clínica que haya permanecido sin movimientos durante 15 años, de acuerdo con lo que se establece en este Decreto. | Art. 21. 2 a 4 del Decreto 38/2012, de 13 de marzo, **País Vasco**, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica |

## 3. ¿CÓMO DEBE OBTENERSE EL CONSENTIMIENTO?

Respecto de este punto, el RGPD si que introduce importantes novedades,

- ✓ El consentimiento debe obtenerse mediante una declaración afirmativa del interesado. Por lo tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

- ✓ Además, el responsable deberá ser capaz de demostrar en todo momento que el titular de los datos otorgó en su momento el consentimiento de tratamiento de datos. Esta obligación implica conservar y/o registrar la cláusula informativa junto con la declaración afirmativa del titular (firma del documento físico o registro del clicado en la página web, por ejemplo).
- ✓ Por otro lado, el titular de los datos puede retirar el consentimiento en cualquier momento, sin justificar el motivo de la retirada.
- ✓ El consentimiento del menor: para tratar datos personales los consentimientos dados por pacientes que tengan 16 años, son plenamente válidos. No obstante lo anterior, los Estados Miembros de la Unión Europea pueden establecer una edad inferior siempre que no sea inferior a 13 años **(España prevé establecer en 13 años la edad para poder consentir los tratamientos de datos en su futura Ley de Protección de Datos).**

## 4. EL REGISTRO DE ACTIVIDADES

El RGPD señala que para que un Responsable pueda demostrar su cumplimiento, debe mantener registros de las actividades de tratamiento bajo su responsabilidad.

Este registro sustituirá la obligación formal que tenían los responsables de inscribir los ficheros en el Registro General de Protección de Datos, como órgano integrado en la Agencia Española de Protección de Datos, depositaria de los registros e inscripciones de los ficheros.

Deberá llevarse dicho registro en determinados supuestos,

- ✓ que el responsable cuente con más de 250 empleados.
- ✓ que el tratamiento realizado pueda entrañar un riesgo para los derechos y libertades de los interesados o que,

- ✓ se realicen tratamientos de datos incluidos en las categorías especiales como son los datos relativos a la salud.

El registro contendrá la siguiente información:

- ✓ El nombre y los datos de contacto del **responsable**.
- ✓ Los **fines** del **tratamiento**.
- ✓ Descripción de las **categorías de interesados** y de las **categorías de datos personales**.
- ✓ Las **categorías de destinatarios**.
- ✓ Las **transferencias** de datos personales a un **tercer país o** una **organización internacional**.
- ✓ Los **plazos de supresión**, cuando sea posible.
- ✓ La **descripción** general de las **medidas técnicas y organizativas de seguridad**, cuando sea posible.

**El registro constará por escrito y se pondrá a disposición de la autoridad de control que lo solicite.**

## 5. ¿QUÉ ES LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO?

El Reglamento busca la aplicación de la protección de datos desde un momento inicial de un proyecto, esto es desde su fase de diseño (Protección desde el diseño).

Por ello, los Responsables deberán garantizar que, por defecto, sólo son objeto de tratamiento los datos necesarios, así como sólo podrán acceder a ellos unas personas físicas determinadas (Protección por defecto).

## 6. LA ADHESIÓN A CÓDIGOS DE CONDUCTA O MECANISMOS DE CERTIFICACIÓN

El RGPD señala que para poder acreditar el correcto cumplimiento por parte de los Responsables se podrán utilizar **mecanismos de certificación o adherirse a Códigos de Conducta.**

Previsiblemente el RGPD traerá mayor desarrollo de estos códigos de conducta a nivel europeo. Estas herramientas deben servir para generar confianza en el cumplimiento de las obligaciones del RGPD, situación que hasta el momento no se estaba produciendo.

## 7. ¿EN QUÉ CONSISTE LA SEGURIDAD DEL TRATAMIENTO?

Con la anterior normativa ya se hacía referencia a la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a la hora de tratar datos personales. Es aconsejable seguir ejecutándolas ya que sirven de base para poder proteger los datos personales que tratemos.

**NIVEL BÁSICO**

| AUTOMATIZADO | MANUAL |
|---|---|
| Funciones y Obligaciones de Personal | Obligaciones Comunes |
| Registro de Incidencias | Criterios de Archivo |
| Control de Acceso | Dispositivos Almacenamiento |
| Gestión de Soportes | Custodia de Soportes |
| Copias de Respaldo y Recuperación | |
| Identificación y Autenticación | |

**NIVEL MEDIO**

| AUTOMATIZADO | MANUAL |
|---|---|
| Responsable de Seguridad | Responsable de Seguridad |
| Auditoría | Auditoría |
| Gestión de Soportes | |
| Identificación y Autenticación | |
| Control de Acceso Físico | |
| Registro de Incidencias | |

**NIVEL ALTO**

| AUTOMATIZADO | MANUAL |
|---|---|
| Gestión y Distribución de Soportes | Almac. de la Información |
| Copias de Respaldo y Recuperación | Copia o Reproducción |
| Registro de Accesos | Acceso a la Documentación |
| Telecomunicaciones | Traslado de la Documentación |

Las medidas de seguridad se encuentran desglosadas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD), todavía en vigor.

Asimismo el RGPD pone de especial relevancia aplicar medidas de seguridad tendentes a,

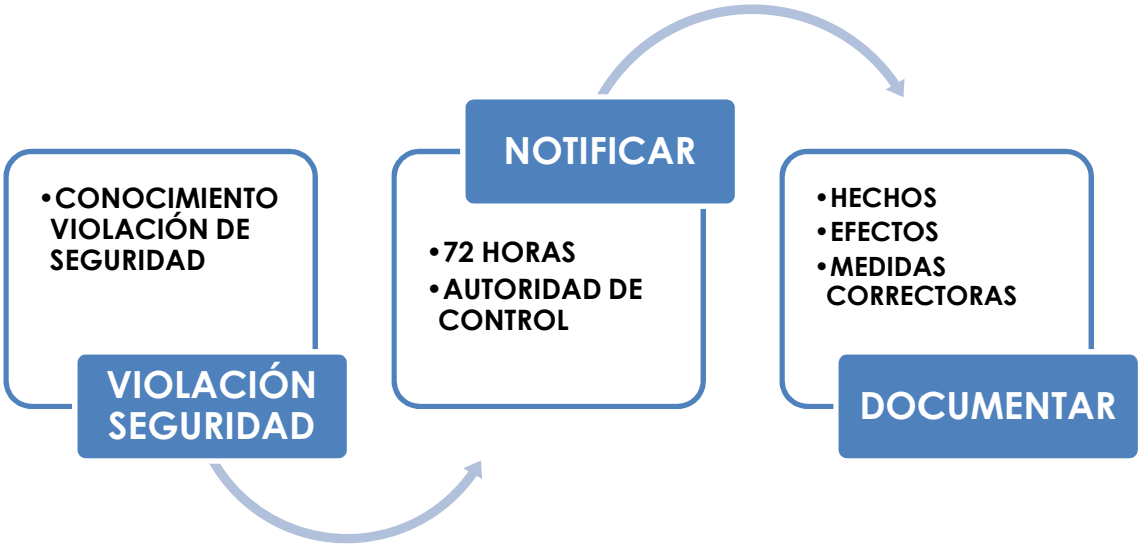
- ✓ La seudonimización y el cifrado de datos.
- ✓ Garantizar la confidencialidad, integridad, disponibilidad y resiliencia.
- ✓ Restaurar la disponibilidad y el acceso a los datos en caso de incidente físico o técnico.

- ✓ Revisar la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

## 8. ¿QUÉ ES UNA NOTIFICACIÓN DE UNA VIOLACIÓN DE SEGURIDAD?

El RGPD entiende por Brecha de Seguridad o violación de seguridad todo aquello que pueda ocasionar la destrucción, pérdida o alteración accidental o ilícita de los datos personales.

El responsable tiene que notificar las violaciones de la seguridad a la autoridad de control competente en un plazo máximo de 72 horas, desde que tuvo conocimiento del hecho.




La notificación incluirá:

- ✓ La naturaleza de la violación de la seguridad, los interesados afectados, y los registros de datos personales afectados.
- ✓ El nombre y datos de contacto del delegado de protección de datos u otro punto de contacto.

- ✓ Las posibles consecuencias.
- ✓ Las medidas adoptadas o propuestas para remediar y/o mitigar los posibles efectos negativos.

**En caso de que la notificación no se produzca en el plazo de 72 horas deberá ir acompañada de los motivos de la dilación.**

## 9. ¿CUÁNDO SE DEBE COMUNICAR LA VIOLACIÓN DE SEGURIDAD AL AFECTADO?

Se deberá comunicar la violación de seguridad al interesado siempre que entrañe un alto riesgo para los derechos y libertades de las personas físicas.

**La autoridad de control podrá exigir la comunicación al interesado si considera que la violación entraña un alto riesgo.**

La comunicación al interesado no será necesaria si se cumplen las siguientes condiciones:

- ✓ Se han adoptado medidas de protección técnicas y organizativas apropiadas y se han aplicado a los datos afectados por la violación.
- ✓ Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de alto riesgo para los derechos y libertades del interesado.
- ✓ Suponga un esfuerzo desproporcionado. En este caso, se optará por una comunicación pública o una medida semejante.

## 10. LA DESIGNACIÓN DE UN DELEGADO DE PROTECCIÓN DE DATOS

La figura del Delegado de Protección de Datos (*Data Protection Officer*, DPO o DPD) es una de las novedades más importantes que contempla el RGPD, y uno de los ejes principales del principio de responsabilidad proactiva.

El DPD deberá ser la persona encargada informar a los responsables o encargados del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos.

Según el RGPD, los Responsables deberán designar un DPD siempre que,

- ✓ el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
- ✓ las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- ✓ las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos (datos salud) o de datos relativos a condenas e infracciones penales.

La definición de "gran escala" se concreta desde Europa como aquellos tratamientos a gran escala de datos sanitarios realizados por parte de un centro hospitalario respecto de sus pacientes.

**España prevé concretar los supuestos en los que será obligatorio designar un DPD en su futura Ley de Protección de Datos).**

El RGPD también establece la designación de un DPD de forma voluntaria siendo esta opción un método de garantía de cumplimiento del RGPD y de responsabilidad proactiva por parte de los Responsables.

**El delegado podrá designarse de forma externa o podrá formar parte de la plantilla del responsable.**

## 11. ¿CÓMO ANALIZAR LOS RIESGOS EN EL TRATAMIENTO DE DATOS?

A fin de poder implantar medidas de seguridad y garantizar los derechos y libertades de las personas, el responsable debe analizar los riesgos inherentes a los tratamientos que efectúa.

Para poder gestionar los riesgos resulta necesario dividir las actuaciones en tres fases[1]

- ✓ **Fase I. Identificación de amenazas.** Acceso ilegítimo a los datos personales (confidencialidad), modificación no autorizada de datos (integridad) y eliminación de datos personales (disponibilidad).
- ✓ **Fase II. Evaluación de riesgos.** Consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice.
- ✓ **Fase III. Tratamiento de riesgos,** o la disminución de los riesgos con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

[1] La AEPD tiene publicada una guía de análisis de riesgos que facilitará la labor a los responsables del tratamiento www.agpd.es

El Responsable deberá documentar las actividades de tratamiento que realiza, teniendo en cuenta toda la vida útil del dato, y bajo el respaldo de su Registro de Actividades.

## 11.1. VIDA ÚTIL DEL DATO PERSONAL

| | |
|---|---|
| **Captura de Datos** | •Cómo se obtienen datos personales (formularios en papel o web, toma de muestras, encuestas, grabaciones de audio o video). |
| **Clasificación y almacenamiento** | •Criterios de organización para poder clasificar y almacenar los datos recogidos (archivos, programas de gestión clínica). |
| **Uso o tratamiento** | •Conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o manuales. |
| **Cesiones o transferencias a terceros** | •Traspaso o comunicación de datos realizada a un terceros. |
| **Destrucción** | •Eliminación de datos, de manera que no puedan ser recuperados de los soportes de almacenamiento |

## 11.2. RIESGOS EN LA ESTRUCTURA QUE LOS ODONTÓLOGOS Y ESTOMATÓLOGOS TRATAN

Teniendo en cuenta las actividades de los odontólogos y estomatólogos la probabilidad de riesgos se ha clasificado de la siguiente forma:

1. Muy bajo (tratamiento sin riesgos)
2. Bajo (tratamiento con pocos riesgos y asumible si se cumple la normativa de protección de datos)
3. Medio (tratamiento susceptible de algún riesgo, que precisa de procesos de verificación de las medidas adoptadas)
4. Alto (tratamiento susceptible de un alto riesgo)
5. Muy Alto (tratamiento con un alto riesgo)

| **POR FINALIDADES** | | |
|---|---|---|
| Gestión de nóminas | Con datos de personas discapacitadas. | 3 |
| Prevención de riesgos laborales | Con historial clínico. | 3 |
| Elaboración de perfiles | Confección de decisiones individuales basadas en un tratamiento automatizado de datos, destinadas a evaluar aspectos personales o a analizar o predecir el rendimiento profesional, situación económica, salud, preferencias o intereses personales, fiabilidad, comportamiento, ubicación o movimientos de una persona. | 3 |
| Publicidad y prospección comercial | Publicidad, venta a distancia, encuestas de opinión, prospección comercial, segmentación de mercados, sistema de ayuda a la toma de decisiones, recopilación de direcciones. | 3 |
| Investigación epidemiológica y actividades analógicas | | 4 |

| | | |
|---|---|---|
| Gestión y control sanitario | | 4 |
| Historial clínico | | 4 |
| **DATOS DE CARÁCTER IDENTIFICATIVO** | | |
| Huella digitalizada | Siempre que permitan la identificación unívoca de la persona. | 4 |
| Marcas físicas | Siempre que permitan la identificación unívoca de la persona. | 4 |
| Datos biométricos | Datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen su identificación única, por ejemplo imágenes faciales, datos dactiloscópicos, etc. | 4 |
| Datos genéticos | Siempre que permitan la identificación unívoca de la persona. | 4 |
| **OTROS DATOS ESPECIALMENTE PROTEGIDOS** | | |
| Vida u orientación sexual | Excepto si los datos se utilizan únicamente en tratamientos no automatizados (papel) de forma incidental o accesoria, sin guardar ninguna relación con su finalidad. | 4 |
| Salud | Excepto si los datos se utilizan únicamente en tratamientos no automatizados (papel) de forma incidental o accesoria, sin guardar ninguna relación con su finalidad, o referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del interesado. | 4 |
| **OTROS DATOS TIPIFICADOS** | | |
| Características personales (personalidad o | Cuando se evalúe la personalidad o el | 3 |

| | | |
|---|---|---|
| comportamiento) | comportamiento de la persona. | |
| Económicos, financieros y de seguro, (si se trata de bancos) | Ingresos y rentas, inversiones y bienes patrimoniales; créditos, préstamos y avales; datos bancarios, planes de pensiones/jubilación, datos económicos de nómina, datos deducciones impositivas/impuestos, seguros, hipotecas, subsidios, beneficios, historial de créditos, tarjetas de crédito. | 3 |
| **TRATAMIENTOS CON PROBABILIDAD DE ALTO RIESGO** | | |
| Utilización de nuevas tecnologías | Cuando se usen nuevas tecnologías que traten datos personales y su naturaleza, alcance, contexto o fines del tratamiento prevean un alto riesgo para los derechos y libertades de los interesados. | 5 |
| Puede vulnerar los derechos y libertades fundamentales de los interesados | Cuando el tratamiento pueda impedir el libre ejercicio de los derechos y libertades de los interesados, o pueda originarles daños y perjuicios materiales o inmateriales. | 5 |
| Se tratan categorías especiales de datos a gran escala | Cuando se trate una considerable cantidad de datos personales que afecten a un gran número de personas con la probabilidad de existir un alto riesgo para sus derechos y libertades. | 5 |
| Evaluación automatizada de aspectos personales (con efectos jurídicos para el interesado) | Cuando sobre cuya base se tomen decisiones que puedan producir efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar (por ejemplo la elaboración de perfiles con datos sensibles). | 5 |

## 11.3. RIESGOS EN EL CUMPLIMIENTO NORMATIVO POR PARTE DE LOS ODONTÓLOGOS Y ESTOMATÓLOGOS

| LEGITIMACIÓN DEL TRATAMIENTO (LICITUD) | | |
|---|---|---|
| Consentimiento EXPLÍCITO para fines determinados | | |
| Consentimiento INEQUÍVOCO mediante una clara acción del interesado | | |
| Para la ejecución de un CONTRATO o precontrato con el interesado | | |
| Tratamiento lícito SIN NECESIDAD DE CONSENTIMIENTO | por un INTERÉS LEGÍTIMO del Responsable del tratamiento o Tercero | |
| | por una OBLIGACIÓN LEGAL del Responsable del tratamiento | |
| | por proceder de una FUENTE LEGÍTIMA DE ACCESO PÚBLICO | |
| | por ser necesario para la protección de los INTERESES VITALES del interesado | |
| | para el cumplimiento de un cometido de INTERÉS PÚBLICO | |
| | por fines de INVESTIGACIÓN histórica, estadística o científica | |
| | por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones | |
| Tratamiento SIN IDENTIFICACIÓN del INTERESADO (seudominización) | CON MEDIDAS adecuadas para que no pueda ser identificado | |
| | SIN MEDIDAS adecuadas para que no pueda ser identificado | 4 |
| Consentimiento TÁCITO (no válido) | | 4 |
| Tratamiento ILÍCITO | | 5 |
| ET | Licitud obtenida mediante la formalización de un CONTRATO de Encargado de tratamiento | |
| ET | Autorización obtenida sin la formalización de un CONTRATO de | 4 |

| | | |
|---|---|---|
| | Encargado de tratamiento | |

| FINALIDAD DEL TRATAMIENTO (LIMITACIÓN DE LOS FINES) | | |
|---|---|---|
| Fines determinados y legítimos | | |
| Fines indeterminados o ilegítimos | | 5 |
| ET | Fines determinados y legítimos | |
| ET | Fines indeterminados o ilegítimos | 5 |

| LIMITACIÓN DEL TRATAMIENTO (MINIMIZACIÓN DE LOS DATOS) | | |
|---|---|---|
| Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS al mínimo para alcanzar los fines | | |
| Obtención de datos DESPROPORCIONADOS para alcanzar los fines | | 5 |
| ET | Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS al mínimo para alcanzar los fines | |
| ET | Obtención de datos DESPROPORCIONADOS para alcanzar los fines | 5 |

| LIMITACIÓN DEL TRATAMIENTO (MINIMIZACIÓN DE LOS DATOS) | | |
|---|---|---|
| EXISTEN PROCEDIMIENTOS para la actualización de datos | | |
| NO EXISTEN PROCEDIMIENTOS para la actualización de datos | | 4 |
| NO SE PUEDEN ACTUALIZAR los datos porqué el fichero no admite manipulación | | |
| ET | EXISTEN PROCEDIMIENTOS para la actualización de datos | |
| ET | NO EXISTEN PROCEDIMIENTOS para la actualización de datos | 4 |
| ET | NO SE PUEDEN ACTUALIZAR los datos porqué el fichero no admite manipulación | |

| LIMITACIÓN DEL TRATAMIENTO (MINIMIZACIÓN DE LOS DATOS) | | |
|---|---|---|
| Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines | | |
| Conservados durante MÁS TIEMPO DEL NECESARIO para alcanzar los fines | por una OBLIGACIÓN LEGAL | |
| | para fines de archivo CON AUTORIZACIÓN del interesado | |
| | para fines de archivo SIN AUTORIZACIÓN del interesado | 4 |
| | para fines de archivo en INTERÉS PÚBLICO | |
| | para fines de INVESTIGACIÓN histórica, estadística o científica | |
| | para otros FINES ILÍCITOS | 5 |
| Conservados INDEFINIDAMENTE mientras exista un INTERÉS MUTUO para mantener el fin del tratamiento | | |
| ET | Conservados SIGUIENDO las instrucciones del Responsable | |
| ET | Conservados SIN SEGUIR las instrucciones del Responsable | 4 |

| PROTECCIÓN DE DATOS (INTEGRIDAD Y CONFIDENCIALIDAD) | | |
|---|---|---|
| EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | | |
| NO EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | | 5 |
| ET | EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | |
| ET | NO EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción | 5 |

| PERSONAL AUTORIZADO | | |
|---|---|---|
| Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | | |
| Los datos son tratados por el PERSONAL de la organización CON UNA OBLIGACIÓN LEGAL fundamentada en la legislación vigente | | |
| Los datos son tratados por el PERSONAL de la organización pero NO EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento | | 4 |
| Los datos son tratados exclusivamente por una ÚNICA PERSONA, la cual es el Responsable del tratamiento | | |
| Los datos son tratados exclusivamente por una ÚNICA PERSONA, la cual es el Encargado del tratamiento | | |
| ET | Los datos son tratados por el PERSONAL de la organización SIGUIENDO LAS INSTRUCCIONES del Responsable del tratamiento | |
| ET | Los datos son tratados por el PERSONAL de la organización CON UNA OBLIGACIÓN LEGAL fundamentada en la legislación vigente | |
| ET | Los datos son tratados por el PERSONAL de la organización SIN SEGUIR LAS INSTRUCCIONES del Responsable del tratamiento | 4 |

| ENCARGADOS DEL TRATAMIENTO (ET) | | |
|---|---|---|
| Los datos NO SON TRATADOS por Encargados del tratamiento | | |
| Los datos SON TRATADOS por Encargados del tratamiento | y EXISTEN CONTRATOS que garantizan medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados | |
| | pero NO EXISTEN CONTRATOS que garantizan medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados | 5 |

| SUBCONTRATACIÓN DEL TRATAMIENTO (SUBET) | | |
|---|---|---|
| ET | NO SE SUBCONTRATA el tratamiento de datos | |

| | | |
|---|---|---|
| ET | SE SUBCONTRATA el tratamiento de datos, CON AUTORIZACIÓN previa y por escrito del Responsable | |
| ET | SE SUBCONTRATA el tratamiento de datos, SIN AUTORIZACIÓN previa y por escrito del Responsable | 4 |

## 11.4. ¿LA REALIZACIÓN DE EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES (EIPD)?

Las Evaluaciones de Impacto relativa a la Protección de Datos personales (EIPD) o *Privacy Impact Assessments (PIAs)* son otra novedad importante en el RGPD.

Las EIPD se justifican también en el principio de *accountability* o principio de responsabilidad proactiva de la organización y encajan perfectamente en la aplicación de medidas de seguridad de protección de datos desde el diseño (*Privacy by Design)*.

Las EIPD serán obligatorias realizarlas en los siguientes supuestos:

| Tratamiento | DPIA | DPO |
|---|---|---|
| El tratamiento puede vulnerar los derechos y libertades fundamentales de los interesados | Cuando el tratamiento pueda impedir el libre ejercicio de los derechos y libertades de los interesados, o pueda originarles daños y perjuicios materiales o inmateriales | |

| | | |
|---|---|---|
| Se utilizan nuevas tecnologías con un alto riesgo para los derechos y libertades de los interesados | Cuando se usen nuevas tecnologías que traten datos personales y su naturaleza, alcance, contexto o fines del tratamiento prevean un alto riesgo para los derechos y libertades de los interesados | |
| Tratamiento a gran escala basado en:<br><br>- Categorías especiales de datos<br><br>- Categorías de datos penales o medidas de seguridad conexas | Cuando se trate una considerable cantidad de datos personales que afecten a un gran número de personas | |
| | Con probabilidad de existir un alto riesgo para sus derechos y libertades | Y la actividad principal de la empresa (a lo que se dedica) es tratar datos personales |
| Tratamiento a gran escala basado en la observación habitual y sistemática de personas | Cuando se realice un seguimiento frecuente y repetitivo de personas con un método de organización, clasificación u ordenación de sus datos | |
| | De zonas de acceso público<br><br>*(Medios de comunicación, Empresas de videovigilancia, Geolocalización, etc.)* | De cualquier zona<br><br>*(Medios de comunicación, Empresas de videovigilancia, Geolocalización, etc.)*<br><br>*(Banca, Aseguradoras, Elaboración de perfiles, ETT, Mercadotecnia directa, Apps, etc.)* |
| Tratamiento basado en una elaboración automatizada de perfiles que pueda afectar a los interesados con efectos | Cuando sobre cuya base se tomen decisiones que puedan producir efectos jurídicos para las | |

| | | |
|---|---|---|
| jurídicos o de alguna otra forma | personas físicas o que les afecten significativamente de modo similar (por ejemplo la elaboración de perfiles con datos sensibles) | |

La Evaluación deberá incluir como mínimo la siguiente información,

- ✓ una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- ✓ una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- ✓ una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
- ✓ las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

## 12. LA CONSULTA PREVIA AL ORGANISMO PERTINENTE.

La consulta previa a la autoridad de control surge también como novedad y como herramienta para prevenir posibles riesgos en la vulneración de los derechos y libertades de las personas físicas.

En situaciones en las que, tras haber realizado una EIPD, el propio tratamiento sigue entrañando un alto riesgo, el responsable del tratamiento podrá realizar una consulta previa a la autoridad de control.

## ¿QUÉ DERECHOS SE RECONOCEN A LOS PACIENTES?

El RGPD en su afán de otorgar más poder de control a los ciudadanos sobre sus datos les reconoce, además de los derechos ya existentes, otros nuevos.

### INFORMACIÓN COMÚN A TODOS LOS DERECHOS:

- ✓ **Plazo de respuesta:** Los derechos ejercitados deberán ser respondidos en el plazo de un mes desde que se recibe la solicitud. Dicho plazo podrá prorrogarse otros dos meses atendiendo a la complejidad y el número de solicitudes. Se deberá informar al interesado de las prórrogas y la motivación de las mismas.

- ✓ **Obligatoriedad de la respuesta:** Los derechos deberán ser contestados SIEMPRE.

- ✓ **Solicitudes infundadas o excesivas:** Para los supuestos de solicitudes infundadas, excesivas o repetitivas se podrá cobrar un canon razonable atendiendo a los costes que representa, o negarse a actuar respecto de la solicitud.

**El Reglamento aumenta el plazo de contestación de todos los derechos a un mes y prevé la posibilidad de exigir el pago de una tasa en caso de ejercicios infundados o excesivos.**

### DERECHO DE ACCESO:

Derecho de los afectados a conocer **si se están tratando o no** sus datos personales y **cuáles** son esos datos.

Se deberá informar sobre:

- ✓ Los **fines** del tratamiento.
- ✓ **Categorías de datos** personales que se traten.
- ✓ Los **destinatarios** de los datos personales.
- ✓ **Derecho** a la **rectificación** o **supresión** de los datos, la **limitación** de su tratamiento y la **oposición** al mismo.
- ✓ **Información del origen** de los datos.
- ✓ La **transferencia** de los datos a un **tercer país** u **organización internacional.**
- ✓ **Plazo de conservación** de los datos personales.
- ✓ **Decisiones automatizadas**, como la elaboración de perfiles.
- ✓ Derecho a presentar una **reclamación**.

## DERECHO DE RECTIFICACIÓN:

El interesado tiene derecho a la **rectificación de los datos personales inexactos** que le conciernan.

## DERECHO DE SUPRESIÓN (DERECHO AL OLVIDO)

El Reglamento incorpora como novedad, junto con el derecho a suprimir los datos, el **derecho al olvido** en Internet.

Este derecho se puede ejercitar cuando la información sea obsoleta o ya no tenga relevancia ni interés público, aunque la publicación original sea legítima.

Debemos recordar que, si se eliminan los datos en el buscador (Google, Yahoo,…), al introducir el nombre del afectado no nos remitirá a dicha información, pero se mantendrá en la Web original.

Los interesados podrán exigir la supresión de sus datos cuando:

- ✓ Los datos personales ya **no** sean **necesarios** atendiendo a los fines para los que fueron recogidos o tratados.
- ✓ Se **oponga** al tratamiento.
- ✓ Así lo exija una **obligación legal**.
- ✓ **Retire su consentimiento**.
- ✓ Los datos personales se hayan obtenido en relación a una **oferta de servicios de la sociedad de la información**.
- ✓ Los datos personales hayan sido **tratados ilícitamente**.

## DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

Es el derecho a **restringir** el tratamiento de los datos personales, mientras éste sea necesario.

Se puede exigir cuando:

- ✓ **Se impugne la exactitud de los datos personales**, mientras se verifica la precisión de los mismos.
- ✓ El responsable ya no **necesite** los datos personales para los fines del tratamiento, pero el interesado los necesite para la **formulación, el ejercicio o la defensa de reclamaciones.**
- ✓ El tratamiento sea **ilícito** y el interesado solicite la limitación en lugar de la **oposición**.
- ✓ Mientras se **verifica la prevalencia de los intereses del responsable** frente a los del interesado, cuando el tratamiento de datos es necesario para la satisfacción de intereses legítimos del responsable.

### DERECHO DE PORTABILIDAD

El Reglamento reconoce el derecho de los **interesados** a recibir los datos personales que le incumban y que éstos sean transmitidos a otro responsable, cuando así lo soliciten.
Se prevén dos **requisitos**:

- ✓ **Consentimiento** del interesado o que sea necesario para la ejecución de un **contrato** en el que éste sea parte;

- ✓ Datos estén **automatizados**.

### DERECHO DE OPOSICIÓN

El interesado podrá oponerse **en cualquier momento** al tratamiento de sus datos personales.

En caso de que un cliente/paciente ejerza este derecho en la Farmacia, deberemos **dejar de tratar los datos,** salvo que acreditemos motivos legítimos que prevalezcan sobre los intereses, derechos y libertades del interesado.

## EL ENCARGADO DEL TRATAMIENTO

### Elección del encargado del tratamiento

El encargado del tratamiento se define como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Una de las grandes novedades que presenta el RGPD es el principio de responsabilidad activa (*accountability*), que viene a imponer al responsable, y al encargado del tratamiento, estar en condiciones de demostrar que cumple con las previsiones normativas en materia de protección de datos de carácter personal.

Según el RGPD, el responsable debe adoptar medidas apropiadas, incluida la elección de encargados, de tal forma que garantice y esté en condiciones de probar que el tratamiento de datos se está realizando conforme a lo que establece el Reglamento Europeo. Esta previsión se extiende igualmente al encargado cuando subcontraten servicios que impliquen acceso a datos, con otros subencargados.

## Responsabilidad del encargado del tratamiento

El RGPD señala que, si un encargado del tratamiento infringe el Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

## Subcontratación

En esencia, para que esta se produzca es necesario que el responsable lo autorice por escrito, bien de forma general o específica.

En el supuesto que la autorización sea de carácter general, el encargado está obligado a informar al responsable de la entrada de un subencargado o

su sustitución por otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

En los supuestos de subcontratación, el encargado debe imponer a ese subencargado, mediante el contrato o acto jurídico, las mismas obligaciones que tiene aquel y que se recogen en el contrato inicial.

En caso de incumplimiento del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

## El contrato de encargo

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.

Como mínimo, en el contrato, acuerdo o acto que regule la relación encargado/responsable debe establecerse,

- ✓ el objeto, duración, naturaleza y la finalidad del tratamiento.
- ✓ el tipo de datos personales y categorías de interesados.
- ✓ la obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable

- ✓ las condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones; la asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

Los contratos de encargo suscritos con anterioridad a la aplicación del RGPD, deben modificarse y adaptarse para respetar el contenido tratado con anterioridad, sin que sean válidas una remisión genérica al artículo del 28 del RGPD.

## ¿QUÉ PODERES TIENE LA AUTORIDAD DE CONTROL?

La autoridad de control es la **autoridad pública e independiente** establecida por un Estado para, entre otras funciones, la supervisión de la aplicación del Reglamento.

Entre sus **poderes** se encuentran:

- ✓ **Sancionar** al responsable con una **advertencia** cuando las operaciones de tratamiento puedan infringir lo dispuesto en el Reglamento.
- ✓ **Sancionar** al responsable con **apercibimiento** cuando las operaciones de tratamiento hayan infringido lo dispuesto en el Reglamento.
- ✓ **Imponer** una **multa administrativa**.

## ¿QUÉ MULTAS PUEDE IMPONER LA AUTORIDAD DE CONTROL?

Las **multas** administrativas se impondrán en **función** de las **circunstancias** de cada caso individual.

Al decidir la multa se tendrá en cuenta:

- ✓ La **naturaleza**, **gravedad** y **duración** de la **infracción**.
- ✓ La **intencionalidad** o **negligencia** en la infracción.
- ✓ Las **medidas** para **paliar** los daños y perjuicios producidos.
- ✓ El **grado de responsabilidad** del responsable.
- ✓ Las **infracciones anteriores** cometidas por el responsable.
- ✓ El grado de **cooperación** con la **autoridad de control**.
- ✓ Las **categorías de datos** de carácter personal afectados.
- ✓ La **forma** en que la **autoridad de control tuvo conocimiento** de la **infracción**, en particular si el responsable notificó la infracción.
- ✓ El **cumplimento** de las **medidas** impuestas por la **autoridad de control con anterioridad**.
- ✓ La **adhesión** a **códigos** de conducta o mecanismos de **certificación**.
- ✓ La aplicación de **cualquier otro** factor **agravante** o **atenuante**.

La infracción de las disposiciones mencionadas a continuación será sancionada con multas administrativas de **10 millones de euros** como máximo o, tratándose de una empresa, de una cuantía equivalente al **2 %** del **volumen del negocio total anual global del ejercicio financiero anterior**, **optándose** por la de **mayor cuantía.**

Multas **10 millones de euros o 2 %** del **volumen**:

- ✓ **Verificar** que el **consentimiento** fue dado o autorizado por el titular de la **patria potestad** o **tutela** sobre el **niño**.
- ✓ **Demostrar** que **no** está en **condiciones de identificar** al interesado, en los casos que el tratamiento no requiere identificación, **e informar cuando sea posible**.
- ✓ **Aplicar** la **protección** de datos **desde el diseño** y **por defecto**.
- ✓ Cumplir las **funciones** del **delegado** de protección de datos.
- ✓ Aplicar las condiciones de la **Certificación**.
- ✓ Cumplir con los requisitos del **Organismo** de **certificación**.

La infracción de las disposiciones enumeradas a continuación será sancionada con multas administrativas de **20 millones de euros** como máximo o, tratándose de una empresa, de una cuantía equivalente al **4 %** del **volumen del negocio total anual global del ejercicio financiero anterior**, **optándose** por la de **mayor cuantía.**

Multas **20 millones de euros o 4 %** del **volumen**:

- ✓ Los **principios básicos** para el tratamiento, incluidas las condiciones para el consentimiento.
- ✓ Los **derechos** de los **interesados**.
- ✓ Las **trasferencias** de **datos** personales a un destinatario en un **tercer país o** una **organización internacional**.
- ✓ Las **obligaciones** adoptadas por los **Estados miembros**.
- ✓ El **incumplimiento** de una **resolución** o de una **limitación** temporal o definitiva del tratamiento o **suspensión** de los flujos de datos por parte de la **autoridad de control**, **o** el **no facilitar** el **acceso**.

# ANEXO I. CLÁUSULA INFORMATIVA DIRIGIDA A PACIENTES

En ……, a fecha .....

…… es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, 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 (Reglamento General de Protección de Datos o RGPD), por lo que se le facilita la siguiente información del tratamiento:

**Fin del tratamiento**: Prestarle el servicio de asistencia sanitaria, seguimiento y evolución (mantenimiento de una historia clínica) así como finalidades derivadas de dicha prestación, incluyendo, entre otras, la gestión administrativa y de facturación y/o recordatorio de citas.

**Criterios de conservación de los datos**: De conformidad con la normativa sanitaria vigente, la documentación se conservará al menos durante **…… años** contados desde la fecha de alta de cada proceso asistencial. Cuando ya no sea necesario para tal fin, se suprimirá la información con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismos.

**Comunicación de los datos**: ***Informar sobre cesiones de datos (Sociedades Médicas, laboratorios, etc..)*** En cualquier otro caso, no se comunicarán los datos a terceros, salvo obligación legal o requerimiento judicial.

**Derechos que asisten al Interesado**: Derecho a retirar el consentimiento en cualquier momento, derecho de acceso, rectificación, portabilidad y supresión de sus datos y a la limitación u oposición a su tratamiento, así como el derecho a presentar una reclamación ante la Autoridad de Control (www.agpd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

**Datos de contacto para ejercer sus derechos:** Podrá ejercitar sus derechos enviando su solicitud junto con un documento acreditativo de su identidad a:

***DATOS DE CONTACTO DEL RESPONSABLE***

***Dirección postal***

***Correo electrónico***

Mediente el presente documento se cumple con el deber de información legal exigido por la normativa de protección de datos y con su firma otorga su consentimiento para el tratamiento de sus datos con los fines arriba expuestos.

☐ ***Si se realizan finalidades accesorias (envío de publicidad y prospección comercial debe detallarse en este apartado en sentido positivo, esto es, AUTORIZO a recibir información sobre productos y/o servicios relacionados con el Responsable.***

Nombre ....., con NIF .....

Representante legal de ....., con NIF .....

Firma:

## ANEXO II. CARTEL INFORMATIVO (MOSTRADOR, RECEPCIÓN)

…… es el **Responsable del tratamiento** de los datos personales del **Interesado** y le informa que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD), por lo que se le facilita la siguiente información del tratamiento:

**Fin del tratamiento**: prestación de servicios profesionales de salud, mantenimiento del historial clínico del Interesado, así como finalidades derivadas de dicha prestación, incluyendo entre otras, la gestión administrativa y de facturación y recordatorio de citas.

**Criterios de conservación de los datos**: De conformidad con la normativa sanitaria vigente, se conservarán al menos durante **…… años** contados desde la fecha del último proceso asistencial. Cuando ya no sea necesario para tal fin, se suprimirá la información con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismos.

**Comunicación de los datos**: ***Informar sobre cesiones de datos (Sociedades Médicas, laboratorios, etc..)*** En cualquier otro caso, no se comunicarán los datos a terceros, salvo obligación legal o requerimiento judicial.

**Derechos que asisten al Interesado**: Derecho a retirar el consentimiento en cualquier momento, Derecho de acceso, rectificación, portabilidad y supresión de sus datos y a la limitación u oposición a su tratamiento, Derecho a presentar una reclamación ante la Autoridad de control (agpd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

**Datos de contacto para ejercer sus derechos:**

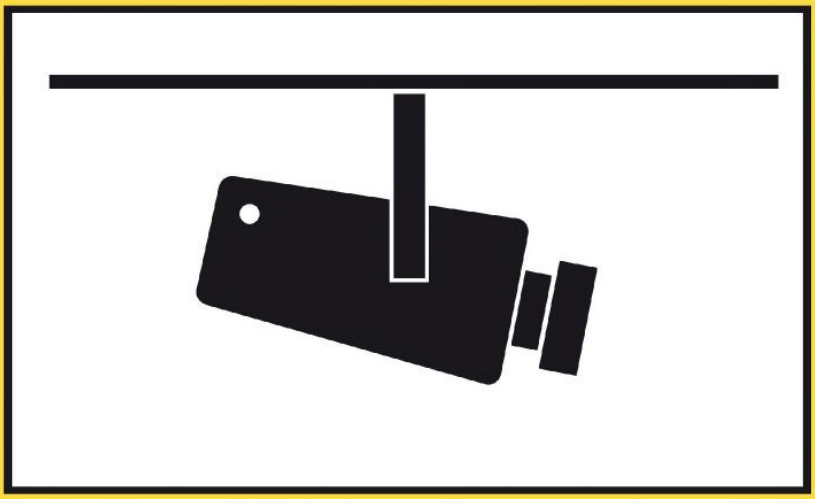
***DATOS DE CONTACTO DEL RESPONSABLE***

***Dirección postal***

***Correo electrónico***

## ANEXO III. CARTEL INFORMATIVO VIDEOVIGILANCIA

# ZONA VIDEOVIGILADA



## PROTECCIÓN DE DATOS

Reglamento (UE) 2016/679 de 27 de abril (GDPR)
Puede ejercer los derechos de acceso, rectificación, supresión, limitación y oposición ante:

Puede presentar una reclamación ante la autoridad de control en agpd.es
Las imágenes se conservarán un máximo de 30 días

# ANEXO IV. REGISTRO DE ACTIVIDADES

| RESPONSABLE DEL TRATAMIENTO<br><br>REGISTRO DE ACTIVIDADES | | |
|---|---|---|
| La obligación de mantenimiento del registro de actividades deriva: | Entidad que emplea a más de 250 personas | |
| | Se realizan tratamientos con riesgo | |
| | Tratamiento no ocasional | |
| | Se realizan tratamientos con categorías especiales de datos personales | |
| | Se realizan tratamientos relativos a condenas e infracciones penales | |
| Formato en el que se mantiene el Registro | En soporte papel | |
| | En soporte electrónico (obligatorio) | x |
| Identificación y contacto | Responsable del tratamiento o del fichero | |

| | | |
|---|---|---|
| | Corresponsable | |
| | Representante | |
| | Delegado de protección de datos | |
| Denominación del tratamiento | | |
| Fecha de inicio del tratamiento | | |
| Finalidad del tratamiento | | |
| Descripción de las categorías | de interesados | |
| | de datos personales | |
| Identificación y descripción de comunicaciones o cesiones de datos | Pasadas o presentes | |
| | Futuras | |
| | Cesionarios en terceros países u organizaciones internacionales | |
| Transferencias internaciones de datos | Identificación del país u organización internacional | |

| | | |
|---|---|---|
| | Supuesto art. 49.1 Excepciones para situaciones específicas. Documentación de garantías adecuadas. | |
| Plazos previstos para la supresión de categorías de datos (en su caso) | | |
| Descripción general de medidas de seguridad | Medidas técnicas | |
| | Medidas organizativas | |

# ANEXO V. FORMULARIO REGISTRO DE BRECHAS DE SEGURIDAD

| MODELO DE REGISTRO, Y EN SU CASO, NOTIFICACION DE UNA VIOLACION DE SEGURIDAD DE DATOS PERSONALES A UNA AUTORIDAD DE CONTROL | | |
|---|---|---|
| | | Fecha: |
| | | Hora: |
| 1.- | Descripción de la violación de seguridad | |
| 2.- | Categorías de datos afectados | |
| 3.- | Número de registros con datos personales afectados | |
| 4.- | Identificación del delegado de protección de datos o persona de contacto.<br><br>Identificación de la persona que detecta la violación de seguridad | |
| 5.- | Fecha y hora en la que se ha detectado la violación de seguridad | |
| 6.- | Posibles consecuencias de la violación de seguridad de datos personales | |
| 7.- | Medidas adoptadas por el responsable del tratamiento | Tecnológicas: |
| | | Organizativas: |
| 8.- | Medidas propuestas por el | Tecnológicas: |

| | | |
|---|---|---|
| | responsable del tratamiento | Organizativas: |
| 9.- | ¿Se trata de una violación de seguridad de los datos con riesgo para los derechos de los afectados? | SI *(continua con la cuestión 10)*<br>NO ( *continua con la cuestión 13)* |
| 10.- | (En su caso) Autoridad de Control a la que notificar la violación de seguridad | *Agencia Española de Protección de Datos* |
| 11.- | (En su caso) Fecha y hora de la notificación a la Autoridad de Control | |
| 12.- | (En su caso) Justificación de la NO notificación de la incidencia en el plazo de 72 horas | |
| 13.- | Identificación de la persona que cumplimenta el presente registro o notificación de la violación. | |

# ANEXO VI. FORMULARIO ATENCIÓN DERECHOS

**FORMULARIOS EJERCICIO DERECHOS**

**(Debe adjuntar copia DNI/NIE/Pasaporte)**

DATOS DEL RESPONSABLE DEL TRATAMIENTO:

RAZÓN SOCIAL:

NIF:

Datos de contacto para ejercer los derechos:

Correo electrónico:

DATOS DEL INTERESADO O REPRESENTANTE LEGAL:

D./ Dª. ..... ..., mayor de edad, con domicilio en..... nº....., Localidad..... C.P..... Provincia..... Comunidad Autónoma..... Teléfono ……..…….. Correo Electrónico: …….. con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho como interesado conforme a los artículos 15, 16, 17, 18, 19, 20, 21, 22 y 23 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD), y en consecuencia, SOLICITA, Que se le facilite gratuitamente el derecho de (marcar con una X solo una casilla):

| | |
|---|---|
| | Acceso a sus datos |
| | Rectificación de sus datos |
| | Supresión de sus datos |
| | Portabilidad de sus datos |
| | Limitación del tratamiento de sus datos |
| | Oposición al tratamiento de sus datos |

| | |
|---|---|
| | No ser objeto de elaboración de perfiles |

Que, conforme al art. 12 del RGPD en el plazo máximo de un mes a contar desde la recepción de esta solicitud (plazo que puede prorrogarse a máximo 2 meses para casos complejos) se responda a la presente solicitud (marcar la casilla correspondiente con una X):

| | |
|---|---|
| | Presencial |
| | Correo ordinario |
| | Correo electrónico |

En Madrid, a _____ de _____de 20____

Fdo:_____

Nombre y Apellidos ....., con NIF .....

Fdo.

Nombre y Apellidos del Representante legal ....., con NIF .....

Ejerce la representación legal de ……

Esta publicación contiene una visión general habiéndose preparado a efectos informativos y no constituye en modo alguno la prestación de un servicio de asesoramiento jurídico ni un medio para establecer una relación profesional ni de ningún otro tipo entre el usuario final y el CGCOE.