Ilustre Colegio Oficial
de Odontólogos y Estomatólogos de la 1ª Región

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

LAS OBLIGACIONES INTRODUCIDAS POR EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. INTRODUCCIÓN.

El próximo 25 de mayo de 2018 entrará en vigor el Reglamento General de Protección de Datos (en adelante **"RGPD"**) que modifica por completo el régimen obligacional establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

A la vista de las importantes sanciones que se prevén en el RGPD[1], es preciso que las **clínicas odontológicas**, como **responsables** del tratamiento de datos personales, se adapten a las exigencias de la nueva regulación y a tal efecto el COEM ha elaborado el presente documento que ofrece una sencilla panorámica de la problemática que la nueva regulación implica.

El cambio primordial es que el RGPD sustituye el actual sistema de comunicación de ficheros a la Agencia Española de Protección de Datos (AEPD) por el **principio de responsabilidad proactiva.** Este principio supone que los responsables de los datos (las clínicas) deben implementar medidas internas tendentes a salvaguardar los datos personales que les hayan sido facilitados.

Es decir, desaparece el deber de comunicación a la AEPD e introduce la obligación de adoptar políticas de protección de los datos en el seno de las empresas para poder acreditar, en caso de eventuales inspecciones, que se garantiza unas exigencias mínimas de protección de los datos personales.

Por otro lado, para que el tratamiento de los datos se ajusta a la nueva legalidad es preciso que el **consentimiento** conferido por los interesados (los pacientes normalmente) **sea expreso y claro.** Por lo tanto, se desecha la posibilidad de tratar datos cuando el consentimiento sea tácito, es decir, cuando no sea claro, expreso e inequívoco.

Asimismo, el contenido de la **información** que se facilita a la hora de recabar el consentimiento de los interesados ha de ser más exhaustiva, incluyendo una serie de extremos que en la normativa actual no son exigibles.

Por último, no debemos olvidar que en el ámbito de la odontología la protección de los datos personales es particularmente sensibles al estar relacionado directamente con **la salud**. Es por ello que, como se indicará posteriormente, este tipo de datos goza de una mayor protección por la normativa aplicable.

[1] El artículo 83.4 del RGPD prevé sanciones máximas de hasta 10.000.000 euros como máximo o, en su caso, la cuantía equivalente a un 2% del volumen de negocio total anual global. Evidentemente, esta cuantía está pensada para grandes empresas multinacionales y será debidamente moderadas de conformidad con el principio de proporcionalidad.

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

2. LAS NUEVAS OBLIGACIONES INTRODUCIDAS POR EL RGPD.

El nuevo RGPD trastoca por completo el sistema de Protección de Datos que estaba implantado en nuestro país ya que suprime la obligación de notificación a la AEPD. De conformidad con la nueva regulación **los responsables han de implementar una serie de medidas** en el seno de su organización para que, en caso de que **sea objeto de inspección**, pueda acreditarse el cumplimiento de las obligaciones de protección.

Para facilitar la comprensión de las obligaciones que introduce el nuevo RGPD se puede dividir en tres grandes grupos las modificaciones en el régimen obligacional introducido por la RGPD: **de información, de consentimiento y la responsabilidad proactiva.**

El deber de información y el modo de recabar el consentimiento para el tratamiento de los datos está prevista en la normativa actual, no obstante, las modificaciones introducidas, si bien no son excesivas, tienen grandes implicaciones prácticas que serán objeto de análisis en sus correspondientes apartados.

El principio de responsabilidad proactiva si constituye un giro drástico de las reglas del juego al modificar por completo el régimen jurídico de la Protección de Datos.

2.1 INFORMACIÓN QUE SE HA DE FACILITAR A LOS PACIENTES.

La **información** que se ha de facilitar tanto a los pacientes como a otras personas físicas cuando se recaba datos de carácter personal ha de incorporar nuevas circunstancias que no están contempladas en la normativa actual. Por consiguiente, el nuevo contenido informativo se tendrá que incluir en el formulario que se facilita a los interesados a la hora de recabar el consentimiento para el tratamiento de datos de carácter personal.

El RGPD[2] establece la información que se debe facilitar al interesado cuando se obtiene datos de carácter personal. Entre otras, se debe facilitar la siguiente información:

a) Se debe facilitar la **identidad y los datos de contacto del responsable** y, en su caso, de su representante. Por lo general, el responsable del tratamiento es la clínica dental, por lo que se deberá facilitar la información sobre su representante legal.
b) En el caso de que la clínica dental cuente con un **delegado de protección**, porque sea obligatorio de conformidad con el RGPD o así lo haya decido el centro odontológico, se deberá facilitar los datos de contacto del mismo.
c) **El fin o los fines** que tendrá el tratamiento de los datos personales y la base jurídica dicho tratamiento.

[2] Artículo 13 del RGPD.

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

d) **Los destinatarios** de los datos personales en su caso.
e) La intención del responsable de **transferir** datos personales a un tercer país.
f) El **plazo de conservación** de los datos personales.
g) El Derecho de los interesados de solicitar al responsable el acceso a sus datos personales, **su rectificación o supresión, la limitación de su tratamiento o la oposición al tratamiento**. Asimismo, se debe informar sobre el derecho a **la portabilidad** de los datos.
h) El derecho a presentar una **reclamación ante una autoridad de control**
i) Que cuando la comunicación de datos personales es un requisito legal o contractual, informar al interesado de la obligación de facilitar de los datos personales y de las posibles consecuencias de no facilitar tales datos.

2.2 CONSENTIMIENTO EXPRESO DE LOS INTERESADOS Y ADECUACIÓN DE LOS FORMULARIOS

El nuevo RGPD introduce las condiciones que ha de reunir el consentimiento de los interesados para que estos sean válidamente otorgados.

El **consentimiento** que se ha de obtener del interesado para que se proceda al tratamiento de los datos de carácter personal **deberá ser expreso** y será preciso indicar específicamente la **finalidad** que tendrá dicho tratamiento. Por lo tanto, el consentimiento tácito dejará de tener validez. Este nuevo requisito tiene una serie de implicaciones prácticas importantes que implicará la modificación de los formularios informativos y para recabar el consentimiento.

En primer lugar, el responsable debe ser capaz de demostrar que el interesado consintió el tratamiento de los datos personales. Para ello, cuando el consentimiento se concede a través de un documento que también hace referencia a otros asuntos, como puede ser el presupuesto de un tratamiento, la solicitud de consentimiento tendrá que presentarse de manera que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso con un lenguaje claro y sencillo.

En segundo lugar, se debe indicar que parte de los datos facilitados por los pacientes en las clínicas son relativos a su **salud**, y este tipo de datos están especialmente protegidos y constituyen una categoría especial de datos a efectos de su tratamiento.

Por lo tanto, en los supuestos que los datos que vayan a ser tratados estén vinculados a la salud, será preciso un consentimiento explícito para el tratamiento de dichos datos personales con una mayor especificación de los fines perseguidos.

En tercer lugar, y es una cuestión de vital importante, se ha de regularizar de cara a eventuales inspecciones el consentimiento de todas las cesiones de datos que se hayan realizado por personas físicas. Tanto aquellas que se obtengan con posterioridad a la entrada en vigor del

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

RGPD como los anteriores. Es decir, **tendrá que obtenerse nuevamente el consentimiento expreso de TODOS datos que no se hayan obtenido de tal manera, aunque se hayan obtenido con anterioridad a la entrada en vigor del RGPD, es decir, antes del 25 de mayo de 2018.**

2.3 EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El **principio de responsabilidad proactiva** – o *accountability* – exige que el responsable del tratamiento, la clínica, establezca **las medidas necesarias** para la debida protección de los datos de carácter personal. Por lo tanto, el responsable deberá demostrar que cumple con las obligaciones derivadas de la normativa y, para ello, deberá implementar medidas de cumplimiento y adopción de una política interna de protección de datos y de privacidad.

El principio de responsabilidad proactiva supone que las clínicas dentales sean capaces de demostrar que cumplen con las obligaciones derivadas de la normativa de protección de datos. Para ello, debe preconstituir una serie de evidencias de cumplimiento y adoptar internamente políticas de privacidad. Destacan una serie de medidas:

1. El principio de *Privacy Design* y *Privacy by Default*:

Este principio implica que los responsables de los Datos deben adoptar políticas internas y otras medidas para que se cumplan las obligaciones en materia de Protección de Datos.

Por lo general se tendrá que elaborar un registro de actividades de tratamiento en el que se inscribirán las operaciones que impliquen un tratamiento de datos, indicando, en función del tipo de la operación:

- La identidad y los datos de contacto del encargado, de los responsables por cuenta del cual actúe y del delegado de protección de datos.
- Las categorías de los tratamientos efectuados por cuenta del responsable.
- Las Transferencias internacionales de datos y documentación de garantías para transferencias de datos internacionales exceptuadas sobre base de intereses legítimos imperiosos.
- Y, en su caso, una descripción general de medidas de seguridad.

Además del registro de actividades de tratamiento, será necesario elaborar manuales internos que permitan desempeñar una correcta gestión de riesgos. Para ello, habrá de identificarse correctamente las tres actividades que constituyen la gestión de riesgos: la identificación de amenazas, la evaluación de riesgos y el tratamiento de los mismos.

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

Por último, y a la luz de la evaluación de las anotaciones del registro de actividades de riesgo y de conformidad con la gestión de riesgos, se introducirán las medidas de seguridad oportunas para reducir o mitigar los riesgos.

Asimismo, los contratos elaborados entre el responsable y el encargado del tratamiento de datos habrán de adecuarse a lo indicado en sus directrices por la Agencia Estatal de Protección de Datos.

2. Evaluación de impacto de la protección de datos:

En determinadas operaciones que conllevan **un alto riesgo** para los derechos de los interesados se debe realizar **una evaluación de impacto a fin de garantizar la seguridad de los datos personales.**

Esta evaluación analizará la naturaleza y la gravedad del riesgo del tratamiento, y a tal efecto, se aplicará medidas apropiadas para mitigarlo.

Un ejemplo paradigmático de la pertinencia de realizar este tipo de evaluaciones de impacto relativo a la protección de datos es el desarrollo de una Aplicación que sea susceptible de recabar un elevado número de datos de carácter personal.

3. Notificación de las brechas de Seguridad de los datos personales:

El responsable estará obligado a notificar a la Autoridad de control, así como a los interesados afectados, de **cualquier violación de la seguridad** de los datos personales **dentro de las 72 de horas desde la producción**. Si bien, no será precisa tal notificación en los supuestos en los que la violación no entrañe un riesgo para los derechos de las personas.

A efectos de cumplimiento de esta obligación, es interesante elaborar un protocolo de actuación cuando se localizan este tipo de brechas susceptibles de vulneración de datos de carácter personal.

4. Nombramiento de un delegado de protección de datos (DPD o DPO).

El Delegado de Protección de Datos es una figura introducida por el RGPD que se erige como garante del cumplimiento de la normativa de la protección de datos de determinadas organizaciones.

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

El Delegado de Protección de Datos deberá contar con conocimientos especializados del Derecho y de protección de datos, y sus funciones son informar, asesorar y supervisar el cumplimiento del RGPD por parte del responsable o encargado.

Será preciso nombrar un Delegado de Protección de **datos cuando las actividades principales del responsable consistan en el tratamiento a gran escala de datos personales de categoría especial, entre los que figuran los datos relativos a la salud.**

En la medida que ni la Unión europea ni la normativa nacional ha especificado que se ha de entender **por tratamiento a gran escala**, la obligación de tener que nombrar un Delegado de Protección por parte de las clínicas dentales no es del todo claro.

En los casos en los que no se asigne un delegado de protección de datos, se tendrá que identificar a la persona responsable de coordinar la adaptación.

5. Garantizar la portabilidad de los datos.

El RGPD reconoce a los interesados el derecho a recibir los datos personales que le incumban que fueron facilitados al responsable y que los transmitan a otro responsable del tratamiento.

Ello implica que los responsables han de tener los medios técnicos y personales para que se pueda transmitir los datos personales a otros responsables cuando sea técnicamente posible.

3. LISTADO DE CONCEPTOS BÁSICOS.

1) **Interesado:**

El interesado es la persona física titular de los datos que son objeto de tratamiento. Por lo general, los interesados son los pacientes de las clínicas dentales, si bien, también lo son las personas que estén vinculadas a los pacientes (supuesto de padres de pacientes menores de edad o tutores legales en caso de pacientes discapacitados), los trabajadores de la clínica, los colaboradores externos…

2) **Datos Personales:**

Toda información sobre una persona física identificada o identificable. Los datos más frecuentes son los nombres y apellidos, dirección de los domicilios, números telefónicos… Asimismo, en el

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

ámbito odontológico otros datos de carácter personal que están especialmente protegidos como son los datos relativos a la salud.

3) **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.

4) **Tratamiento:**

Cualquier operación realizada sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, conservación, consulta, utilización, difusión…

5) **Responsable del tratamiento**:

Es la persona física o jurídica, que determina los fines y medios del tratamiento. En nuestro caso, las clínicas odontológicas son responsables del tratamiento de los datos que se obtengan de las personas. Asimismo, el propio COEM sería responsable del tratamiento de los datos de sus colegiados, de sus trabajadores…

6) **Encargado del tratamiento:**

Es la persona física o jurídica que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento. Esta prestación se formaliza a través de un contrato escrito entre el responsable del tratamiento y el encargado.

7) **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.

8) **Violación de la seguridad de los datos personales:**

Es 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.

Mauricio Legendre, 38 - 28046 Madrid
Teléfono 91 561 29 05 - Fax 91 563 28 30
www.coem.org.es

9) **Fichero:**

Es el conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.