REGISTRO DE ACTIVIDADES DE TRATAMIENTO

ILUSTRE COLEGIO PROFESIONAL DE PROTESICOS DENTALES DE ARAGON

C/ Vicente Berdusan, Bloque D-1 Bajos

50010-ZARAGOZA

Q5000448J

Documento en actualización permanente.

ÍNDICE

1.- OBJETO DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

2.- IDEINTIFICACION DE INTERVINIENTES

3.- IDENTIFICACIÓN Y DESCRIPCIÓN DE TRATAMIENTOS

4.- DESCRIPCIÓN DE LAS MEDIDAS DE SEGURIDAD A APLICAR TRAS LA INICIAL EVALUACIÓN DE RIESGOS

1.- OBJETO DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El presente documento (Registro de Actividades de Tratamiento, en adelante RAT), tiene por objeto dar cumplimiento a lo establecido en el Art. 30 del Reglamento Europeo de Protección de Datos UE 679/2016, de 27 de abril, del Parlamento y el Consejo (RGPD), en el art. 31 de la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), y en el resto de la normativa nacional vigente, y para ello se realizan las siguientes operaciones:

1º.- Realizar una identificación completa del Responsable del Tratamiento y, en su caso, del Corresponsable, del Representante del Responsable (en caso de que el Responsable del Tratamiento no tuviera su establecimiento en España), y del Delegado de Protección de Datos, señalando los datos de contacto de los mismos.

2º.- Realizar una descripción de las categorías de interesados y de las categorías de datos personales que se hayan incluido y sean tratados en el sistema de tratamiento de datos de la entidad ILUSTRE COLEGIO PROFESIONAL DE PROTESICOS DENTALES DE ARAGON como Responsable del Tratamiento.

3º.- Realizar una descripción de las finalidades de los distintos tratamientos de datos.

4º.- Realizar una descripción de las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

5º.- Realizar una descripción de las comunicaciones de datos a terceros, cuando estos actúen en calidad de Encargados de Tratamiento o Cesionarios, si los hubiere.

6º.-En el caso de producirse una transferencia internacional de datos a un tercer país u organización internacional, realizar una descripción de: los destinatarios, los datos transferidos, el tercer país u organización internacional de que se trate y la justificación de las garantías adecuadas.

7º.- Cuando sea posible, determinar los plazos previstos para la supresión de las diferentes categorías de datos.

8º.- Cuando sea posible, realizar una descripción general de las medidas técnicas y organizativas de seguridad establecidas en el art. 32, apartado 1 del RGPD: la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; disponer de un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Mediante la realización de una Evaluación de Riesgos se analizaron los posibles riesgos inherentes al Tratamiento llevado a cabo por el Responsable.

En el caso de ser necesaria una Evaluación de Impacto (EIPD), adicionalmente se determinará el daño que se puede producir para la confidencialidad, integridad y seguridad de los datos que dicho Responsable ha de garantizar, y se establecerán las medidas que se recomienda adoptar para evitar o minimizar riesgos y daños (art. 35 RGPD).

2.- IDENTIFICACION DE INTERVINIENTES

RESPONSABLE DEL TRATAMIENTO

ILUSTRE COLEGIO PROFESIONAL DE PROTESICOS DENTALES DE ARAGON

CIF: **Q5000448J**

DIRECCIÓN: **C/ Vicente Berdusan, Bloque D-1 Bajos. 50010-ZARAGOZA**

TÉFONO.: **976460332**

C. ELECTRÓNICO: **coppda@coppda.com**

WEB: **www.coppda.com**

CORRESPONSABLE **SIN CORRESPONSABLE**

DENOMINACION:

DATOS DE CONTACTO:

REPRESENTANTE **SIN REPRESENTANTE**

DENOMINACION:

DATOS DE CONTACTO:

DELEGADO PROTECCION DE DATOS

DENOMINACION: **PROTECCIÓN DE DATOS Y PREVENCIÓN, S.L.**

DATOS DE CONTACTO: **C/ Doctor González Caraballo, 1. 41020-SEVILLA. dpo@pdyp.es**

3.- IDENTIFICACIÓN Y DESCRIPCIÓN DE TRATAMIENTOS

Se han identificado como tratamiento todas aquellas operaciones que se realizan, automatizadas o no, y finalidades de dichas operaciones, teniendo en cuenta los distintos colectivos de titulares de datos de carácter personal con los que se relaciona el Responsable del Tratamiento.

A continuación se exponen los nombres de los distintos tratamientos que se llevan a cabo por la entidad y se detallan as características de cada uno de ellos.

EMPLEADOS

COLEGIADOS

JUNTA DE GOBIERNO

CANAL DE DENUNCIAS

EMPLEADOS

- Categoría de Interesados:

Empleados

Solicitantes

- Legitimación del Tratamiento

Consentimiento del interesado (RGPD: 6.1.a); Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte (RGPD: 6.1.b)

.Descripción de la Finalidad:

Recursos Humanos

Gestión de Nóminas

- Categoría de Datos

NIF; Nº.SS/Mutualidad; Nombre y Apellidos; Dirección; Teléfono; Características personales; académicos y profesionales; detalles de empleo; Económicos, financieros y de seguros;

- Origen de los datos

El propio Interesado o su representante legal

- Cesión de datos

Organismos de la Seguridad Social; Administración Tributaria; Bancos, Cajas de ahorros y cajas Rurales; entidades aseguradoras

- Transferencias Internacionales de Datos

Sin transferencias Internacionales de datos

- Plazos previstos para la supresión de los datos

Se conservarán hasta su prescripción legal

- Sistema de Tratamiento: MIXTO

- Titularidad Tratamiento: PRIVADO

- Nivel de Seguridad a aplicar: BASICO

COLEGIADOS

- Categoría de Interesados:

Colegiados; Solicitantes

- Legitimación del Tratamiento

Consentimiento del interesado (RGPD: 6.1.a); Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte (RGPD: 6.1.b); Satisfacción de intereses legítimos perseguidos por el responsable del tratamiento (RGPD: 6.1.f); Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (RGPD: 6.1.c); Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (RGPD: 6.1.e)

.Descripción de la Finalidad:

Otras finalidades

Relación integral con los Colegiados

- Categoría de Datos

NIF/CIF; Nombre y Apellidos; Dirección; Teléfono Académicos y Profesionales; Detalles de Empleo; Información Comercial

- Origen de los datos

El propio interesado o su representante legal; Registros públicos

- Cesión de datos

Organizaciones o personas relacionadas directamente con el responsable;Registros públicos; Colegios profesionales; Administración tributaria;Otros órganos de la Administración Pública; Bancos, cajas de ahorro y cajas rurales; Entidades aseguradoras; Administación pública con competencia en la materia

- Transferencias Internacionales de Datos

Sin transferencias Internacionales de datos

- Plazos previstos para la supresión de los datos

Se conservarán hasta su prescripción legal

- Sistema de Tratamiento: MIXTO

- Titularidad Tratamiento: PUBLICO

- Nivel de Seguridad a aplicar: BASICO

JUNTA DE GOBIERNO

- Categoría de Interesados:

Colegiados; Solicitantes

Asociados o miembros

- Legitimación del Tratamiento

Consentimiento del interesado (RGPD: 6.1.a); Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte (RGPD: 6.1.b); Satisfacción de intereses legítimos perseguidos por el responsable del tratamiento (RGPD: 6.1.f); Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (RGPD: 6.1.c); Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (RGPD: 6.1.e)

.Descripción de la Finalidad:

Otras finalidades

Relación integral con los miembros de la Junta de Gobierno

- Categoría de Datos

NIF/CIF; Nombre y Apellidos; Dirección; Teléfono Académicos y Profesionales; Detalles de Empleo; Información Comercial

NIF/DNI; Nombre y Apellidos; Dirección; Teléfono

Académicos y Profesionales

- Origen de los datos

El propio interesado o su representante legal; Registros públicos

El propio interesado o su representante legal

- Cesión de datos

Organizaciones o personas relacionadas directamente con el responsable;Registros públicos; Colegios profesionales; Administración tributaria;Otros órganos de la Administración Pública; Bancos, cajas de ahorro y cajas rurales; Entidades aseguradoras; Administación pública con competencia en la materia

Organizaciones o personas relacionadas directamente con el responsable

- Transferencias Internacionales de Datos

Sin transferencias Internacionales de datos

- Plazos previstos para la supresión de los datos

Se conservarán hasta su prescripción legal

- Sistema de Tratamiento: MIXTO

- Titularidad Tratamiento: PRIVADO

- Nivel de Seguridad a aplicar: BASICO

CANAL DE DENUNCIAS

- Categoría de Interesados:

Denunciantes; Denunciados; Clientes y usuarios,; proveedores; Empleados; Solicitantes; Asociados o Miembros

- Legitimación del Tratamiento

Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (RGPD: 6.1.c); Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (RGPD: 6.1.e)

.Descripción de la Finalidad:

Gestión del procedimineto de la ley 2/2023, en su Art. 9

- Categoría de Datos

DNI/NIF; Nombre y Apellidos; Dirección; Correo electrónico; Teléfono; Firma

- Origen de los datos

El propio interesado o su representante legal; otras personas físicas

- Cesión de datos

Administración pública con competencia en la materia; Fuerzas y Cuerpos de Seguridad; Organizaciones o personas relacionadas directamente con el Responsable; Juzgados; Otros órganos de la Administración pública

- Transferencias Internacionales de Datos

Sin transferencias Internacionales de datos

- Plazos previstos para la supresión de los datos

Se conservarán hasta su prescripción legal

- Sistema de Tratamiento: MIXTO

- Titularidad Tratamiento: PRIVADO

- Nivel de Seguridad a aplicar: BASICO

4.- DESCRIPCION DE LAS MEDIDAS DE SEGURIDAD A APLICAR TRAS LA EVALUACIÓN DE RIESGOS

De acuerdo con lo estipulado en el art. 35 del RGPD, será imprescindible realizar una evaluación de impacto cuando concurran algunas de las siguientes circunstancias:

1.- Que el tratamiento de datos tenga por objeto la elaboración de perfiles y análisis automatizado de aspectos personales.

2.- Que se trate de un tratamiento a gran escala de categorías especiales de datos personales.

3.- Que el objetivo sea una observación sistemática a gran escala de zonas de acceso público.

Independientemente de que exista la obligación legal o no de realizar una Evaluación de Impacto, y en aplicación del principio de Responsabilidad Proactiva que le incumbe al Responsable, se han determinado las medidas técnico-organizativas que se consideran necesarias adoptar, tras la inicial evaluación de riesgos realizada, con el objetivo de eliminar o minimizar los riesgos que entraña el Tratamiento de Datos de Carácter Personal para la seguridad de la información (integridad, confidencialidad-privacidad y disponibilidad de los mismos).

Se han determinado dos niveles de medidas a aplicar a cada uno de los Tratamientos incluidos en este Registro. Se les han denominado Básico y Alto.

Los criterios principales que se han tenido en cuenta, para determinar el nivel que le corresponde a cada Tratamiento, han sido, entre otros:

a) Si se trata de datos englobados en los denominados Datos de Categoría Especial.

b) Si el Tratamiento de datos lo lleva a cabo más de una persona.

c) Si hay cesiones o comunicaciones de datos a terceros.

d) Necesidad de realizar una EIPD.

e) En general, el art. 32 RGPD establece: “Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el Responsable y el Encargado del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”.

CATEGORIAS DE COLECTIVOS, Y NIVEL DE SEGURIDAD A APLICAR PROPUESTO

COLECTIVO	S. TRATAMIENTO	N. SEGURIDAD
EMPLEADOS	MIXTO	BASICO
COLEGIADOS	MIXTO	BASICO
JUNTA DE GOBIERNO	MIXTO	BASICO
CANAL DE DENUNCIAS	MIXTO	BASICO

MEDIDAS DE SEGURIDAD A APLICAR EN TODOS LOS NIVELES

TRATAMIENTOS AUTOMATIZADOS/NO AUTOMATIZADOS

Funciones y obligaciones de los usuarios

Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el Registro de Actividades de Tratamiento. -Definir las funciones de control o autorizaciones delegadas por el Responsable del Tratamiento. -Formación e información de los usuarios para que conozcan de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en las que pudiera incurrir en caso de incumplimiento.

Usuarios y control de acesos

Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones. -Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. -Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. -Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el Registro de Actividades de Tratamiento, conforme a los criterios establecidos por el Responsable del Tratamiento. -El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Registro de incidencias

Establecer un procedimiento de notificación y gestión de las incidencias. -Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Gestión de soportes y documentos

Etiquetado

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. -No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. - Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.

Registro de salida

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico,

fuera de los locales bajo el control del Responsable del Tratamiento deberá ser autorizada por el Responsable del Tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.

Traslado

En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Destrucción

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Control de Acceso físico

Exclusivamente el personal autorizado en el Registro de Actividades de Tratamiento podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Controles periódicos de verificación

La veracidad de los datos contenidos en el Registro de Actividades de Tratamiento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías que supongan un riesgo en el cumplimiento de la Ley Orgánica de Protección de Datos Personales.

TRATAMIENTOS AUTOMATIZADOS

Identificación y autenticación

Adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. -Establecer mecanismos para la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. -Si se usan contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. -El Registro de Actividades de Tratamiento establecerá un cambio periódico de contraseñas nunca superior a un año. Mientras estén vigentes, se almacenarán de forma ininteligible. - El Responsable del Tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Copias de respaldo y recuperación

Copia de respaldo

Copia de respaldo con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. -Fijar procedimientos para la recuperación de los datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. -En ficheros parcialmente automatizados si existe

documentación que permite la reconstrucción se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Registro de Actividades de Tratamiento.

Control periódico

Control periódico semestral de la definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Pruebas con datos reales

Prohibición de pruebas con datos reales anteriores a la implantación o modificación de los sistemas de información salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el Registro de Actividades de Tratamiento. Deberá haberse realizado una copia de seguridad.

Registro de incidencias: recuperación de datos

El registro deberá consignar, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesario grabar manualmente en el proceso de recuperación. -Será necesaria la autorización del Responsable del Tratamiento para la ejecución de los procedimientos de recuperación de los datos.

TRATAMIENTOS NO AUTOMATIZADOS

Gestión de Soportes y Documentos

Etiquetado

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. -No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. -Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.

Registro de salida

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del Responsable del Tratamiento deberá ser autorizada por el Responsable del Tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.

Traslado

En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su

transporte.

Destrucción

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Custodia de Soportes

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el Responsable del Tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Dispositivos de almacenamiento

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Criterios de Archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el Responsable del Tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.