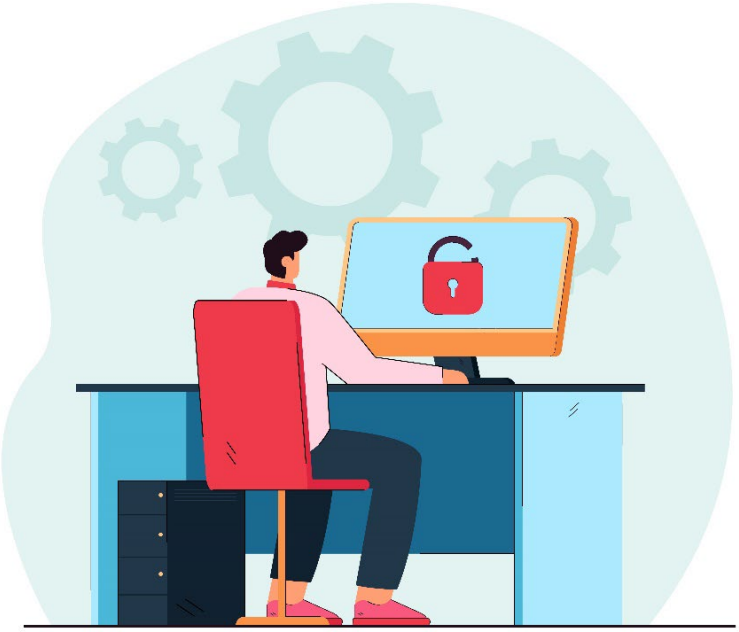
apdcat
Autoritat Catalana de Protecció de Dades

Guía de protección de datos para los colegios profesionales y consejos de colegios

Actualización: junio 2024

Col·lección guías. Núm. 6



Generalitat de Catalunya

Índice

Presentación

La Autoridad Catalana de Protección de Datos, en el marco del Convenio de colaboración con la Asociación Intercolegial, ha elaborado esta Guía de protección de datos para los colegios profesionales y los consejos de colegios recogiendo los cambios normativos producidos a raíz de la plena aplicación, a partir del día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos - RGPD) y la posterior aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El RGPD obliga tanto a los responsables del tratamiento como a las autoridades de protección de datos a ser proactivos en su actuación a la hora de garantizar el tratamiento adecuado de los datos personales. Por ello, esta Guía quiere ofrecer una visión amplia de la normativa de protección de datos que permite no sólo dar solución a los problemas más frecuentes con que se encuentren los colegios profesionales, sino también detectarlos y dar una solución antes de que se produzcan.

El objeto de esta guía no es sustituir los textos normativos de aplicación, que son los que en cualquier caso determinan de forma detallada el contenido de las obligaciones del responsable del tratamiento, sino recoger de una forma general, sistematizada y comprensible los aspectos más relevantes a la hora de tratar datos personales. También ofrecer criterios orientadores que los colegios profesionales deben tener en cuenta en su actuación diaria, con el fin de adecuarla a lo que establece la normativa de protección de datos personales.

Para hacerlo, en cada uno de los apartados de la Guía se recoge en primer lugar un resumen de los aspectos más relevantes de la normativa aplicable, que se complementa con una serie de preguntas y respuestas frecuentes, con indicación de la normativa aplicable más relevante en cada apartado. Aunque, para simplificar la lectura, en esta guía a menudo se hará referencia solamente a los colegios profesionales, las consideraciones que contiene son extensibles a los consejos de colegios profesionales.

Espero que os sea una herramienta útil para garantizar de una manera efectiva los derechos y las libertades de las personas afectadas.

Meritxell Borràs i Solé
Directora

1. Marco normativo

- Reglamento (UE) núm. 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.[1]
- 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.[2]
- Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos.
- Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos.
- Instrucción 1/2009 de la Agencia Catalana de Protección de Datos, de 10 de febrero de 2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.[2]
- Recomendación 1/2008 de la Autoridad Catalana de Protección de Datos, sobre la difusión de información que contenga datos de carácter personal a través de Internet.

También conviene tener en cuenta las siguientes guías publicadas por la APDCAT:

- Guía para el cumplimiento del deber de informar en el RGPD
- Guía sobre el encargado del tratamiento en el RGPD
- Guía práctica sobre la evaluación de impacto relativa a la protección de datos
- Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD (publicación del núm. de DNI)
- Lista de tipos de operaciones de tratamiento que deben someterse a EIPD

[1] Los artículos 23 y 24 siguen siendo aplicables en el ámbito del RGPD.
[2] Aplicable en aquello que no sea contrario al RGPD y la LOPDGDD.

2. Conceptos clave

Afectado: persona física titular de los datos personales sometidos a tratamiento.

En esta guía se utiliza el término *persona afectada* y no *interesado*, que utiliza el RGPD, con el fin de evitar confundirlo con el concepto de interesado que regula la normativa del procedimiento administrativo.

Anonimización: tratamiento de datos que produce la ruptura de la cadena de identificación de la persona afectada, de forma que los datos ya no se puedan atribuir a una persona física identificada o identificable.

Categorías especiales de datos: datos personales que, por su naturaleza, reciben una protección especial dado su carácter sensible en relación con los derechos y libertades fundamentales de los afectados y los riesgos que pueden derivarse de su tratamiento.

Forman parte de estas categorías:

- Las opiniones políticas.
- Las convicciones religiosas o filosóficas.
- La afiliación sindical.
- Los datos que revelan el origen étnico o racial.
- Los datos genéticos.
- Los datos biométricos destinados a identificar de manera unívoca a una persona física.
- Los datos relativos a la salud.
- Los datos relativos a la vida sexual o a la orientación sexual de una persona física.

Los datos relativos a infracciones y condenas penales y las relativas a infracciones y sanciones administrativas no se consideran categorías especiales de datos, aunque ambas categorías cuentan con un régimen específico que introduce algunas restricciones a su tratamiento.

Datos personales: cualquier información sobre una persona física identificada o identificable. En consecuencia, la normativa de protección de datos no afectará a la información relativa a personas jurídicas o cuando es anónima, es decir, cuando no se puede relacionar con una persona física.

La protección de datos personales abarca todos los aspectos de la vida de una persona física. Por eso, por ejemplo, en el caso de los profesionales liberales o de los empresarios individuales puede abarcar también aspectos de su vida profesional.

Se considera **persona identificable** la persona que puede ser identificada directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un

número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

La normativa de protección de datos personales no se aplica a los datos de las personas difuntas.

Destinatario: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al cual se comunican datos personales, tanto si es un tercero como si no.

> No se consideran destinatarios los encargados del tratamiento, ni las autoridades públicas que pueden recibir datos personales en el marco de una investigación concreta.
>
> Tampoco el personal propio de los colegios profesionales, cuando accede a los datos personales en ejercicio o desarrollo de sus funciones.

Elaboración de perfiles: cualquier forma de tratamiento automatizado de datos personales consistente en el uso de los datos para evaluar determinados aspectos de una persona física; en especial, para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de esta persona.

Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trata datos personales por cuenta del responsable del tratamiento.

Fuentes accesibles al público: actualmente, la normativa de protección de datos no contiene una definición de qué hay que entender como fuente accesible al público, ni establece ningún régimen específico con respecto al tratamiento de los datos que pueden contener. Se puede considerar como fuente de acceso público cualquier conjunto de información de libre acceso para la ciudadanía.

Responsable del tratamiento: persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o junto con otros, determina las finalidades y los medios del tratamiento.

Pueden ser responsables de los respectivos tratamientos los colegios profesionales, cualquiera de sus órganos o entes instrumentales o entidades sin personalidad jurídica que actúen en el tráfico jurídico como sujeto diferenciado.

Puede haber más de un responsable del tratamiento. En este caso, hay que determinar las responsabilidades de cada uno en un acuerdo establecido a este efecto, atendiendo a las actividades que efectivamente lleva a cabo cada uno de los **corresponsables** del tratamiento.

Seudonimización: tratamiento de los datos personales de forma que ya no se puedan atribuir a un afectado sin utilizar información adicional, siempre que esta información conste por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.

Los datos personales **seudonimizados**, que se pueden atribuir a una persona física utilizando información adicional, como por ejemplo un código, se consideran información sobre una persona física identificable.

Tercero: persona física o jurídica, autoridad pública, servicio u organismo diferente de la persona afectada, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea mediante procedimientos automatizados o no, como la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, careo o interconexión, limitación, supresión o destrucción.

¿El tratamiento de los datos relativos a las sociedades profesionales del colegio está dentro del ámbito de aplicación de la normativa de protección de datos?

El RGPD y la LOPDGDD sólo se aplican a los datos de personas físicas. Por lo tanto, no lo sería respecto de los datos de una sociedad profesional. Ahora bien, las sociedades profesionales están formadas o gestionadas por personas físicas (socias, representantes, administradoras, etc.), respecto de las cuales sí que son de aplicación el RGPD y la LOPDGDD.

¿Una dirección de correo electrónica facilitada por el colegio a una persona colegiada es un dato personal?

Los colegios profesionales pueden adoptar diferentes criterios en la confección de las direcciones de correo electrónico que facilitan a sus colegiados (direcciones personalizadas, no personalizadas o direcciones genéricas). Si la dirección de correo electrónico se puede asociar directa o indirectamente a una persona física, es un dato

personal cuyo tratamiento debe adecuarse a los principios y las garantías de la normativa de protección de datos.

Normativa aplicable: art. 4, 9, 10 y 26 RGPD; 10 y 27 LOPDGDD.

3. El tratamiento de datos en los colegios profesionales

En ejercicio de las funciones que tienen encomendadas, los colegios profesionales y los consejos de colegios profesionales tienen que tratar como responsables del tratamiento numerosos datos personales de diferentes colectivos, como los de las personas colegiadas, del personal del colegio, de los proveedores, de las personas asistentes a actividades u otras personas con las cuales se relacionan. Estos datos pueden ser de distintas tipologías (identificativas, de características personales, de formación, profesionales, económicas, de menores, etc.).

En el caso de los colegios profesionales es importante tener en cuenta que, en algunos aspectos previstos en la normativa de protección de datos, el régimen aplicable puede depender de si el colegio está actuando en ejercicio de funciones públicas o funciones privadas. Eso será relevante, por ejemplo, a la hora de determinar la base jurídica (consentimiento, misión en interés público, interés legítimo, etc.); la obligación de incorporar un tratamiento al inventario de actividades de tratamiento; la posibilidad de ejercer el derecho a la portabilidad; la exigibilidad de la aplicación del Esquema Nacional de Seguridad; el régimen sancionador aplicable; etc.

La normativa reguladora de los colegios profesionales determina que son **funciones públicas** de los colegios profesionales las siguientes:

- Garantizar que el ejercicio profesional se adecue a la normativa, la deontología y las buenas prácticas y que se respeten los derechos y los intereses de las personas destinatarias de la actuación profesional.
- Velar por los derechos y por el cumplimiento de los deberes y las obligaciones de los colegiados y para que no se produzcan actos de intrusismo, de competencia desleal u otras actuaciones irregulares.
- Ejercer la potestad disciplinaria sobre sus colegiados, en los términos establecidos por la ley y las normas propias de los colegios profesionales.
- Visar los proyectos y los trabajos de las personas colegiadas, en los términos y con los efectos que establece la normativa correspondiente.
- Participar en el procedimiento de obtención de la acreditación de aptitud para ejercer la profesión colegiada, si la ley establece este requisito.
- Promover y facilitar la formación continua de las personas colegiadas que permita garantizar su competencia profesional.

- Adoptar las medidas necesarias para facilitar el ejercicio profesional no permanente, en cumplimiento de lo que establecen la normativa de la Unión Europea y las leyes.
- Colaborar con la Administración pública mediante la participación en órganos administrativos, cuando así se prevea legalmente, y emitir los informes que los órganos o autoridades administrativos y judiciales les requieran.
- Informar sobre los proyectos de disposiciones generales que afecten al ejercicio de la profesión o la institución colegial.
- Fomentar el uso de la lengua catalana entre las personas colegiadas y en los ámbitos institucionales y sociales en los que se ejerce la profesión.
- Informar en los procesos judiciales y administrativos en los que se discutan cuestiones relativas a honorarios y aranceles profesionales.
- Aprobar sus presupuestos y regular y fijar las aportaciones de los colegiados.
- El resto de funciones de naturaleza pública que les atribuye la legislación vigente o que les haya delegado una administración pública.

En cambio, son **actividades privadas** de los colegios profesionales:

- Fomentar y prestar servicios en interés de las personas colegiadas y de la profesión en general.
- Gestionar el cobro de las remuneraciones y de los honorarios profesionales a petición de las personas colegiadas, de acuerdo con lo que establecen los estatutos respectivos.
- Intervenir, por vía de mediación o de arbitraje, en los conflictos profesionales entre personas colegiadas o entre estas y terceras personas, siempre que lo soliciten de común acuerdo las partes implicadas.
- Colaborar con las asociaciones y otras entidades representativas de los intereses de los ciudadanos directamente vinculadas con el ejercicio de la profesión colegiada.
- Facilitar información en materia de honorarios profesionales, respetando siempre el régimen de libre competencia.
- Custodiar, a petición del profesional o la profesional y de acuerdo con los estatutos, documentación propia de su actividad que se vean obligados a guardar de conformidad con la normativa vigente.
- Otras no vinculadas al ejercicio de potestades públicas.

A la hora de tratar los datos, los colegios profesionales deben tener en cuenta los principios que establece la normativa de protección de datos, y que se exponen con más detalle en los apartados siguientes de esta guía:

- **Principios de licitud, lealtad y transparencia:** los datos deben tratarse de forma lícita, leal y transparente en relación con la persona afectada.
- **Principio de limitación de la finalidad:** los datos deben recogerse con finalidades determinadas, explícitas y legítimas y posteriormente no deben tratarse de forma incompatible con estas finalidades.

- **Principio de minimización de datos:** los datos tienen que ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las cuales se tratan.
- **Principio de exactitud:** los datos tienen que ser exactos y, si es necesario, actualizados.
- **Principio de limitación del plazo de conservación:** los datos deben conservarse sólo durante el período necesario para las finalidades del tratamiento.
- **Principio de integridad y confidencialidad:** los datos deben tratarse de forma que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.
- **Principio de responsabilidad proactiva** *(accountability)***:** el responsable del tratamiento es responsable del cumplimiento de estos principios y tiene que ser capaz de demostrarlo.

De acuerdo con estos principios, los colegios profesionales deben tener en cuenta una serie de elementos para garantizar que el tratamiento se lleva a cabo en condiciones adecuadas:

Primero: concretar la finalidad del tratamiento.

Segundo: identificar la base jurídica del tratamiento.

Tercero: tratar y utilizar únicamente los datos necesarios para alcanzar la finalidad.

Cuarto: establecer garantías adecuadas en la prestación de servicios por cuenta del colegio profesional que impliquen el tratamiento de datos personales.

Quinto: atender los derechos de las personas afectadas.

Sexto: cumplir las obligaciones que prevé el RGPD. Eso incluye la obligación del responsable del tratamiento de aplicar las medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento es conforme a la normativa de protección de datos, teniendo en cuenta la naturaleza, el ámbito, el contexto y las finalidades del tratamiento, así como los riesgos de probabilidad y gravedad diversa para los derechos y las libertades de las personas físicas.

Incluye, como mínimo, las obligaciones siguientes:

- Facilitar información sobre el tratamiento de los datos a las personas afectadas.
- Llevar el registro y el inventario de actividades del tratamiento.
- Designar un delegado de protección de datos.
- Aplicar la protección de datos desde el diseño y por defecto.
- Velar por la exactitud y la actualización de los datos.
- Velar por la seguridad de los datos: integridad y confidencialidad.

- Hacer la evaluación de impacto relativa a la protección de datos y la consulta previa, si procede.
- Aprobar una política de protección de datos, si procede.

Estas medidas deben revisarse y actualizarse cuando sea necesario.

Séptimo: adoptar otras medidas proactivas para garantizar los derechos y libertades de las personas afectadas, si procede.

Octavo: velar que se ofrezcan garantías adecuadas en las transferencias internacionales de datos.

Noveno: velar por la conservación adecuada de los datos.

Es importante que el colegio profesional, como responsable del tratamiento, esté en disposición de poder demostrar que se han adoptado medidas para garantizar las condiciones adecuadas de los tratamientos, ya sea a través de protocolos, procedimientos, instrucciones internas, documentación, registros, actividades de formación, comunicaciones, etc. Es lo que se conoce como responsabilidad proactiva o *accountability*. En los apartados siguientes de esta guía se ofrecen orientaciones básicas para cumplir estos aspectos.

¿Cómo se puede determinar si la finalidad de un tratamiento está vinculada al ejercicio de funciones públicas?

Hay que ver si la finalidad se puede incluir dentro de alguna de las funciones públicas que les atribuye la normativa reguladora de los colegios profesionales (Ley 7/2006) u otra normativa. Por otra parte, la jurisprudencia también ha reconocido que hay diferentes actividades de los colegios que hay que considerar funciones públicas, como las cuestiones relativas a la defensa de la corporación, la constitución de sus órganos, su régimen electoral o las decisiones sobre colegiación y disciplina, la aprobación de sus presupuestos o también las cuestiones relativas a los visados colegiales.

¿Y en el caso de los tratamientos de datos que llevan a cabo los consejos de colegios?

Como en el caso de los colegios profesionales, hay que ver si la finalidad se puede incluir dentro de alguna de las funciones públicas que les atribuye la normativa reguladora de los colegios profesionales (Ley 7/2006) u otra normativa.

¿Qué naturaleza tiene el tratamiento de datos de precolegiados?

Puede considerarse de naturaleza pública, en la medida que los datos personales que se incorporan se recogen con vistas al procedimiento de incorporación en el colegio como colegiados. De lo contrario, si la finalidad del tratamiento se refiere a actividades que no están reguladas como funciones públicas del colegio, hay que considerarla de naturaleza privada.

4. Las finalidades del tratamiento

Los datos personales deben recogerse con finalidades determinadas, explícitas y legítimas, y no pueden tratarse posteriormente de manera incompatible con las finalidades iniciales para las que se recogieron. Por eso es importante que, antes de iniciar la recogida, el responsable del tratamiento establezca claramente la finalidad y la haga constar tanto en el registro de actividades del tratamiento, como en la información que debe facilitar a las personas afectadas.

Se consideran compatibles los tratamientos de los datos con finalidades de archivo en interés público, de investigación científica e histórica o con finalidades estadísticas. No obstante, será necesario adoptar garantías adecuadas para las personas afectadas y, en particular, garantizar el respeto al principio de minimización. Para cumplir este principio se pueden utilizar medidas como la seudonimización o incluso la anonimización, siempre que permitan alcanzar la finalidad del tratamiento. En los tratamientos que se lleven a cabo con estas finalidades, la ley puede establecer excepciones a los derechos de las personas afectadas.

Una nueva finalidad (finalidad posterior o secundaria) también se puede considerar compatible, cuando el nuevo tratamiento se basa en el consentimiento de las personas afectadas o en el derecho de la Unión o de un estado miembro con alguno de los objetivos que recoge el artículo 23 del RGPD (seguridad del estado, defensa, seguridad pública, prevención, investigación, detección o enjuiciamiento de infracciones penales o deontológicas, ejecución de sanciones penales, objetivos importantes de interés público, protección de la persona afectada o de los derechos y libertades de otros, o ejecución de demandas civiles).

Más allá de estos supuestos, el responsable del tratamiento puede determinar que el uso de los datos con una finalidad secundaria es compatible con la finalidad inicial, teniendo en cuenta, entre otras, las circunstancias siguientes:

- La relación entre las finalidades iniciales y las posteriores.
- El contexto en que se han recogido los datos, en particular con respecto a la relación entre las personas afectadas y el responsable.
- La naturaleza de los datos personales, en concreto si se trata de categorías especiales de datos o de datos relativos a condenas e infracciones penales.
- Las consecuencias del tratamiento posterior para las personas afectadas.
- La existencia de garantías adecuadas, como el cifrado la seudonimización.

En estos casos, hay que informar a las personas afectadas de la nueva finalidad o finalidad secundaria. También del resto de aspectos previstos en el RGPD, a menos que ya hayan sido informadas previamente.

Normativa aplicable: considerando 50, art. 5.1.*b)*, 6.4, 13.3 y 89.1 RGPD.

5. La licitud del tratamiento

El RGPD establece que todo tratamiento de datos personales tiene que ser lícito. Eso significa que, además de respetar las leyes, como cualquier otra actividad de los colegios profesionales, sólo se puede llevar a cabo si se fundamenta en alguna de las bases jurídicas que establece el artículo 6.1 del mismo RGPD.

Estas bases jurídicas no mantienen entre sí ninguna relación de prioridad o prelación y un mismo tratamiento puede contar con más de una base jurídica.

La elección de la base jurídica del tratamiento debe hacerse siempre antes de empezar las operaciones de tratamiento, teniendo en cuenta su finalidad, y hay que incluirla en la información que se facilita a la persona afectada.

En el caso de los colegios profesionales, cuando ejerzan funciones públicas normalmente la base jurídica será el ejercicio de una misión en interés público o el ejercicio de potestades públicas. A veces también puede ser, por ejemplo, el cumplimiento de una obligación legal o la ejecución de un contrato.

El consentimiento de las personas afectadas, si bien no se puede descartar con carácter general, será un supuesto poco habitual, teniendo en cuenta que la situación de desigualdad existente, por lo menos cuando se ejercen funciones públicas, entre la posición jurídica del colegio profesional y la de la ciudadanía o la persona colegiada que se relaciona con él, puede condicionar el carácter libre del consentimiento.

Cuando ejerzan funciones privadas, la habilitación basada en el consentimiento puede tener un papel más importante. En estas funciones, también hay que tener en cuenta la habilitación derivada de la consecución de un interés legítimo.

En el caso de las categorías especiales de datos, su tratamiento está prohibido con carácter general, a menos que, además de una de las bases jurídicas del artículo 6.1, concurra alguna de las excepciones del artículo 9.2 del RGPD.

5.1 Las bases jurídicas del tratamiento

Para el cumplimiento del principio de licitud, el RGPD prevé diferentes bases jurídicas en las cuales se puede basar la legitimidad del tratamiento:

- El consentimiento de la persona afectada.
- El tratamiento es necesario para ejecutar un contrato en el cual la persona afectada es parte, o bien para aplicar medidas precontractuales a petición suya.

- El tratamiento es necesario para cumplir una obligación legal aplicable al responsable del tratamiento.
- El tratamiento es necesario para proteger intereses vitales de la persona afectada o de otra persona física.
- El tratamiento es necesario para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El tratamiento es necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no prevalezcan los intereses o los derechos y las libertades fundamentales de la persona afectada.

¿Un colegio profesional puede tratar datos personales recogidos de páginas web de terceros (números de teléfono, direcciones electrónicas personales, nombres y apellidos, etc.)?

No, a menos que se disponga de alguna de las bases jurídicas previstas en el RGPD.

5.1.1 El consentimiento de la persona afectada

El consentimiento constituye una de las seis bases jurídicas establecidas en el RGPD en las que el responsable puede fundamentar el tratamiento de datos personales.

El consentimiento sólo es una base jurídica adecuada si reúne los requisitos establecidos en la normativa de protección de datos. En concreto, el consentimiento de la persona afectada debe ser:

Informado. Antes de que la persona afectada otorgue el consentimiento, hay que facilitarle la información suficiente para que comprenda qué está consintiendo realmente.

En este sentido, tiene especial importancia la información sobre la identidad del responsable y las finalidades del tratamiento, sin perjuicio de los otros aspectos a los cuales nos referiremos en el apartado relativo a la información a las personas afectadas.

Libre. La persona afectada tiene que disponer de una capacidad de elección y control real, de modo que si decide no dar el consentimiento o retirarlo no se deriven consecuencias negativas o perjuicios de ningún tipo.

No se puede considerar que el consentimiento ha sido prestado libremente cuando:

- Hay un desequilibrio evidente entre la persona afectada y el responsable del tratamiento, en particular cuando este responsable es una autoridad pública. Los colegios profesionales deben tenerlo especialmente en cuenta cuando ejercen funciones de carácter público.

- No permite autorizar por separado las diferentes operaciones de tratamiento de datos, a pesar de ser adecuado en el caso concreto.
- La ejecución de un contrato se supedita al consentimiento para tratar datos que no son necesarios para el contrato mencionado.

> Con carácter general, el consentimiento no es válido si se ejerce cualquier influencia o presión inadecuada sobre la persona afectada que le impida actuar libremente de acuerdo con su voluntad.
>
> Estas influencias o presiones inadecuadas pueden manifestarse de formas muy diversas, según el contexto y las características propias del tratamiento de datos.

Específico. El consentimiento se puede requerir para todas las actividades de tratamiento que responden a una misma finalidad concreta y determinada.

Si el tratamiento tiene varias finalidades, el consentimiento debe requerirse de forma separada para cada una de ellas (consentimiento granular).

Inequívoco. La persona afectada tiene que otorgar su consentimiento mediante un acto afirmativo claro o una manifestación de voluntad de aceptar el tratamiento de datos que le afectan.

Además de inequívoco, el consentimiento tiene que ser **explícito** en los supuestos siguientes:

- Tratamiento de categorías especiales de datos.
- Toma de decisiones individuales automatizadas.
- Transferencias internacionales de datos.

> El llamado consentimiento “tácito”, basado en la inacción de la persona afectada o en el uso de casillas premarcadas, no es admisible.
>
> En cambio, sí es conforme al RGPD el uso de una declaración por escrito o la marcación de casillas en un sitio web.
>
> Si se utiliza una declaración escrita que también haga referencia a otros asuntos, la parte referida a la protección de datos tiene que quedar claramente diferenciada del resto de declaraciones.

La persona afectada tiene derecho a retirar el consentimiento en cualquier momento, del mismo modo, o más sencillo, que la fórmula utilizada para darlo, sin que eso afecte a la licitud del tratamiento previo a la revocación basado en el consentimiento.

Corresponde al responsable demostrar en todo momento que la persona afectada ha otorgado el consentimiento y que éste es válido.

> Los tratamientos de datos iniciados por los colegios profesionales antes de la aplicación del RGPD basados en el consentimiento de la persona afectada siguen siendo lícitos, si el consentimiento se prestó con los requisitos que establece el RGPD. En especial, conviene revisar si se prestó mediante una manifestación o acción afirmativa clara.

El consentimiento de los menores de edad

Si la persona afectada es menor de edad, hay que tener presente que el tratamiento de sus datos sólo se puede fundamentar en su consentimiento si tiene más de 14 años. Eso, a menos que se trate de supuestos en que una ley exija la asistencia del titular de la potestad parental o tutela para llevar a cabo el acto o el negocio jurídico en el contexto del cual se solicita el consentimiento.

En este caso, hay que explicar en un lenguaje claro y sencillo para los menores de edad de qué manera se tratarán los datos personales.

En caso de menores de edad de menos de 14 años, el tratamiento de datos fundamentado en el consentimiento requiere el consentimiento del titular de la potestad parental o tutela.

¿Los colegios profesionales pueden utilizar el consentimiento como base jurídica de los tratamientos de datos que llevan a cabo?

Es posible, aunque normalmente el consentimiento no es la base jurídica en la cual pueden ampararse los tratamientos de datos que se llevan a cabo en el ejercicio de funciones públicas de los colegios profesionales. En el ámbito de las administraciones públicas, cuando actúan en ejercicio de sus competencias, el ciudadano no siempre está en condiciones de poder negar su consentimiento de una manera libre. Por eso, normalmente la base jurídica es la relativa al cumplimiento de una misión de interés público o el ejercicio de poderes públicos.

En cambio, en sus funciones privadas la pueden utilizar normalmente. Algunos ejemplos en que podría operar el consentimiento serían la suscripción a un servicio ofrecido por el colegio, como una actividad lúdica, la suscripción a su página web para recibir comunicaciones sobre determinados productos o la inscripción en una bolsa de trabajo, entre otros.

¿Cómo puede probar el responsable del tratamiento el consentimiento de la persona afectada a un tratamiento específico?

El RGPD establece la obligación explícita del responsable de demostrar que la persona afectada ha dado su consentimiento, pero no prescribe cómo tiene que hacerlo. Así, los responsables del tratamiento tienen libertad para escoger el medio

que permita cumplir con esta obligación. En este sentido, hay que tener en cuenta las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 del Comité Europeo de Protección de Datos (CEPD), adoptadas el 4 de mayo de 2020.

Si se tienen que tratar categorías especiales de datos (art. 9 RGPD), el consentimiento debe ser explícito.

¿Cómo hay que actuar si se pierde la documentación donde se había recogido el consentimiento de la persona afectada para tratar sus datos?

Si no se dispone de otra base jurídica, el colegio profesional tiene que cesar en el tratamiento de datos hasta obtener nuevamente el consentimiento de la persona afectada, el cual debe reunir los requisitos establecidos en el RGPD. Si se quiere fundamentar en otra base jurídica, las personas afectadas tienen que ser informadas de la nueva base jurídica y tienen que poder ejercer los derechos inherentes a esta nueva base jurídica.

¿Un colegio profesional puede, sobre la base jurídica del consentimiento, utilizar grupos de un servicio de mensajería instantánea para comunicarse con los colegiados?

Sí, siempre que, con respecto a las funciones públicas, los participantes tengan otros canales alternativos de comunicación con el colegio para las finalidades previstas; es decir, que este servicio no se les imponga como única vía de comunicación. En todo caso, hay que contar con el consentimiento de todas las personas integrantes del grupo.

Hay que velar para que el servicio cumpla con las medidas de seguridad adecuadas, teniendo en cuenta la finalidad de las comunicaciones para las cuales se utilizará.

¿Sigue siendo válido el consentimiento otorgado antes de la entrada en vigor del RGPD?

Sí, siempre que reúna los requisitos establecidos por el RGPD, es decir, que el consentimiento sea informado, libre, específico e inequívoco. De lo contrario, el colegio tiene que cesar en el tratamiento hasta obtener nuevamente el consentimiento de la persona afectada, a menos que cuente con alguna otra base jurídica.

Normativa aplicable: considerandos 32, 38, 42 y 43 y art. 4.11), 6.1.a), 7, 8, 9.2.a), 22.2.c) y 49.1.a) RGPD; art. 6, 7 y 9 LOPDGDD.

5.1.2 La ejecución de un contrato

El RGPD considera lícito el tratamiento de datos cuando es necesario para ejecutar un contrato en que la persona afectada es parte o para aplicar medidas precontractuales a petición de esta persona.

¿Los colegios profesionales pueden tratar los datos de su personal laboral sobre la base jurídica relativa a la ejecución de un contrato?

Sí, siempre que estos datos sean necesarios para mantener o cumplir la relación laboral que estos trabajadores tienen con el colegio o con alguno de los entes que dependen de él.

Normativa aplicable: considerandos 40 y 44 y art. 6.1 *b)* RGPD.

5.1.3 El cumplimiento de una obligación legal

De acuerdo con el RGPD, el tratamiento de datos también puede ser lícito cuando es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Es necesario que esta obligación esté prevista en una norma con rango de ley o en el derecho de la Unión Europea.

¿Un colegio profesional puede comunicar los datos de sus trabajadores a la Tesorería General de la Seguridad Social, al solicitar la afiliación de un trabajador a la Seguridad Social?

Sí, dado que la legislación sectorial aplicable establece expresamente la obligación del empresario, en este caso del colegio, de solicitar la afiliación de quien ingrese en su servicio.

Normativa aplicable: considerandos 41 y 45 y art. 6.1.c) RGPD; art. 8.2 LOPDGDD.

5.1.4 La protección de intereses vitales

El RGPD también permite el tratamiento de datos cuando es necesario para proteger un interés esencial para la vida de la persona afectada o de otra persona física.

En principio, esta base jurídica tiene carácter subsidiario, es decir, sólo tiene que utilizarse cuando el tratamiento de datos no se puede fundamentar en ninguna otra de las bases jurídicas. Esta base jurídica también puede ser aplicable a situaciones como el tratamiento de datos con finalidades humanitarias, incluido el control y la propagación de epidemias, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Normativa aplicable: considerando 46 RGPD; art. 6.1.*d)* RGPD.

5.1.5 El cumplimiento de una misión de interés público o en el ejercicio de poderes públicos

El RGPD permite el tratamiento de datos personales cuando es necesario para cumplir una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

La misión de interés público o, si procede, los poderes públicos mencionados tienen que derivar de una función atribuida al colegio por una norma con rango de ley.

La legislación que regula los colegios profesionales les atribuye una serie de funciones públicas. Por ejemplo, garantizan que el ejercicio de la profesión se adecue a la normativa, la deontología y las buenas prácticas; ejercen la potestad disciplinaria sobre los colegiados; visan los proyectos y los trabajos; regulan y fijan las aportaciones colegiales; y promueven la formación continua de los colegiados para garantizar la competencia profesional. Sobre esta cuestión, nos remitimos al apartado 3 de esta guía.

Para ejercer estas y otras funciones públicas que tienen encomendadas, los colegios pueden recoger y tratar determinados datos de las personas colegiadas y de terceras personas, sin requerir el consentimiento.

¿Un colegio profesional puede difundir en el portal web y por redes sociales fotografías de acontecimientos organizados por el colegio donde aparezcan personas físicas, sin su consentimiento?

La difusión de imágenes de personas físicas que ocupen un cargo público o una profesión de proyección pública, o de personas que aparecen como meramente accesorias, en actos o acontecimientos organizados por el colegio vinculados a sus funciones públicas puede tener base jurídica suficiente, siempre de acuerdo con lo que dispone la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y a la propia imagen. Eso, sin perjuicio de que se aplique el principio de minimización y se informe adecuadamente a las personas afectadas.

Cuando las imágenes estén vinculadas al ejercicio de sus funciones privadas, puede contar con la base jurídica derivada de la existencia del interés legítimo.

¿Un colegio profesional puede pedir a una universidad que confirme si una determinada persona colegiada, o que ha pedido colegiarse, tiene la titulación habilitante para hacerlo?

Sí. En este caso, la base jurídica se encontraría en el artículo 6.1.e) en relación con la normativa que les atribuye el control del ejercicio de la profesión y la disposición adicional octava de la LOPDGDD.

Normativa aplicable: considerando 45 y art. 6.1.e) RGPD; art. 8.2 LOPDGDD; art. 5 y 7 Ley 2/1974; art. 39 y s. y 51 Ley 7/2006.

5.1.6 La satisfacción de un interés legítimo

El tratamiento de datos personales también puede ser lícito cuando es necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no deban prevalecer los intereses o los derechos y las libertades fundamentales de la persona afectada que requieren la protección de datos personales, especialmente si la persona afectada es un niño. A estos efectos, el responsable del tratamiento tiene que llevar a cabo la ponderación apropiada.

Los colegios profesionales pueden utilizar esta base jurídica en el ejercicio de sus funciones privadas.

En cambio, los colegios profesionales no pueden utilizar esta base jurídica para fundamentar los tratamientos de datos que llevan a cabo en ejercicio de sus funciones públicas. No obstante, esta base jurídica puede fundamentar la comunicación de datos personales solicitados por otros sujetos en los cuales concurra un interés legítimo que deba prevalecer sobre los derechos e intereses de las personas afectadas. En este caso, para poder aplicar esta base jurídica, el colegio profesional tiene que hacer una ponderación y apreciar en estas personas un interés legítimo que deba prevalecer sobre los derechos e intereses de las personas afectadas.

Para hacer la ponderación de intereses y determinar si concurre un interés legítimo que pueda fundamentar el tratamiento de los datos, hay que tener en consideración tres factores:

- El interés legítimo del responsable o de terceros.
- El impacto del tratamiento sobre las personas afectadas.
- Las garantías adicionales que se apliquen a los tratamientos.

¿Un colegio profesional puede enviar información a sus colegiados, por correo postal, sobre un nuevo servicio de carácter privado que ofrece el colegio, o sobre productos y servicios ofrecidos por terceros, al amparo de la base jurídica del interés legítimo?

Este tratamiento, que se podría considerar una actividad de marketing directo, se podría basar en el interés legítimo. Eso, a menos que la persona colegiada se haya opuesto, se haya inscrito en un sistema de exclusión publicitaria o que de la ponderación de las circunstancias concurrentes resulte que debe prevalecer el derecho a la protección de datos de las personas afectadas.

Si la comunicación se hace por medios electrónicos, resulta de aplicación el régimen especial configurado por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico.

De acuerdo con este régimen, las comunicaciones comerciales por medios electrónicos tienen que contar con el consentimiento expreso de las personas

afectadas, excepto los supuestos en que exista una relación comercial previa y la comunicación se refiera a productos o servicios de su propia empresa similares a los que se contrataron inicialmente.

Normativa aplicable: considerando 47 y art. 6.1.*f)* RGPD; art. 23 y DA 10 LOPDGDD.

5.2 Las categorías especiales de datos

El RGPD establece un régimen más restrictivo para tratar determinados datos, que, por su naturaleza, son particularmente sensibles, dado que su tratamiento podría implicar grandes riesgos para los derechos y libertades de las personas afectadas. En concreto, se establece una prohibición general de tratamiento respecto de las categorías siguientes:

- Las opiniones políticas.
- Las convicciones religiosas o filosóficas.
- La afiliación sindical.
- Los datos que revelan el origen étnico o racial.
- Los datos genéticos.
- Los datos biométricos destinados a identificar de manera unívoca a una persona física.
- Los datos relativos a la salud.
- Los datos relativos a la vida sexual o a la orientación sexual de una persona física.

A pesar de eso, el mismo RGPD establece una serie de excepciones en las cuales se pueden tratar estas categorías de datos. En el caso de los colegios profesionales, conviene destacar las siguientes:

- El tratamiento se fundamenta en el consentimiento explícito de la persona afectada. Hay que tener en cuenta que el mero consentimiento de la persona afectada puede no ser suficiente para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, cuando pueda dar lugar a situaciones discriminatorias.
- El tratamiento es necesario para cumplir obligaciones o ejercer derechos en el ámbito laboral, si así lo autoriza el derecho de la Unión o del estado miembro. El derecho del estado miembro puede consistir en una norma con rango de ley o en un convenio colectivo.
- El tratamiento es necesario para proteger intereses vitales de la persona afectada o de otra persona física, en el supuesto de que la persona afectada no esté capacitada físicamente o jurídicamente para dar el consentimiento.
- El tratamiento se refiere a datos personales que la persona afectada ha hecho manifiestamente públicos.

- El tratamiento es necesario para formular, ejercer o defender reclamaciones o cuando los tribunales actúan en ejercicio de su función judicial.
- El tratamiento es necesario por razones de un interés público esencial, establecido en una ley o en el derecho de la Unión, que tiene que ser proporcional al objetivo perseguido, respetar el derecho a la protección de datos en lo esencial y establecer medidas adecuadas y específicas para proteger los intereses y los derechos fundamentales de la persona afectada.
- El tratamiento es necesario para finalidades de medicina preventiva o laboral, de evaluación de la capacidad laboral del trabajador, de diagnóstico médico, de prestación de asistencia o de tratamiento de tipo sanitario o social, o de gestión de los sistemas y los servicios de asistencia sanitaria y social, sobre la base de una norma con rango de ley o del derecho de la Unión o en virtud de un contrato con un profesional sanitario.
  Este tipo de tratamiento tiene que efectuarlo un profesional sujeto al deber de secreto o bien bajo su responsabilidad, o cualquier otra persona sujeta a la obligación de secreto.
- El tratamiento es necesario con finalidades de archivo en interés público, con finalidades de investigación científica o histórica o con finalidades estadísticas, sobre la base de una norma con rango de ley o derecho de la Unión que regule garantías adecuadas para los derechos y libertades de las personas afectadas.

> La concurrencia de alguna de las circunstancias previstas en el artículo 9 RGPD no exime de la necesidad de disponer de una base jurídica de las previstas en el artículo 6 RGPD, sino que actúa de manera cumulativa.

En relación con el tratamiento de datos genéticos y de datos relacionadas con la salud, hay que tener en cuenta lo que dispone la disposición adicional decimoséptima de la LOPDGDD.

Los responsables o encargados que traten estos tipos de datos deben tener en cuenta especialmente esta circunstancia, cuando analicen los riesgos derivados del tratamiento. Además, si los tratan a gran escala, tienen determinadas obligaciones específicas como hacer una evaluación de impacto, o determinados requisitos específicos cuando quieran tomar decisiones automatizadas, incluida la elaboración de perfiles.

A pesar de no formar parte de las categorías especiales de datos, los datos relativos a condenas e infracciones penales, así como los relativos a procedimientos y medidas cautelares y de seguridad conexas, sólo se pueden tratar al amparo de una norma de derecho de la Unión o en una norma con rango de ley. Únicamente se puede llevar un registro completo de estos datos bajo el control de las autoridades públicas y de conformidad con lo que establece la regulación del sistema de registros administrativos de apoyo a la Administración de justicia.

Con respecto a los datos relativos a infracciones y sanciones administrativas, no tienen la condición de categoría especial de datos, aunque tienen un régimen específico. Al respecto, nos remitimos al apartado 5.4.1 de esta guía.

¿Se pueden utilizar datos biométricos para el control horario en el entorno laboral y para el acceso a determinadas dependencias?

Dado que el RGPD ha incluido los datos biométricos dentro de las categorías especiales de datos, es necesario que exista una norma con rango de ley o un convenio colectivo que lo prevea expresamente. En estos casos no se puede concluir de manera general que sea adecuado utilizar estos sistemas, sino que es necesario que, previamente, el responsable del tratamiento realice una evaluación de impacto sobre la protección de datos para evaluar la proporcionalidad, las garantías y las medidas de seguridad previstas.

¿Es necesario que el colegio profesional realice una evaluación de impacto relativa a la protección de datos para tratar datos de salud en la gestión de recursos humanos?

En principio, si el tratamiento que se lleva a cabo sólo implica la recogida de datos relativos a situaciones de bajas de los trabajadores, discapacidades, accesibilidad o prevención de riesgos laborales, necesarios para cumplir con las obligaciones establecidas en la normativa vigente, no parece que sea exigible por este hecho una evaluación de impacto relativa a la protección de datos.

¿Un colegio profesional puede facilitar datos al departamento competente en materia de salud de la Generalitat de Catalunya, con la finalidad de control de epidemias?

Sí, el RGPD habilita que las autoridades en materia de salud pública traten datos personales, incluidas categorías especiales de datos, como los datos de salud, "cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección ante amenazas transfronterizas graves para la salud, o para garantizar niveles elevados de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del derecho de la Unión o de los estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y las libertades de la persona afectada, en particular el secreto profesional" (artículos 6.1.e) y 9.2.i) RGPD). A estos efectos hay que tener en cuenta las previsiones de la Ley 14/1986, de 25 de abril, General de Sanidad; la Ley 33/2011, de 4 de octubre, General de Salud Pública; la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública; y la Ley 18/2009, del 22 de octubre, de salud pública.

El desarrollo de estas actuaciones puede comportar que las autoridades en materia de salud pública recojan información, incluidos datos de salud relativos a personas contagiadas o sospechosas de estarlo y que, si procede, la revelen cuando sea estrictamente necesario para aplicar medidas de control.

Normativa aplicable: considerandos 34, 35, 51 a 56, 71 y art. 9, 10 y 22.4 RGPD; art. 9.1, 10, DA 17ª, DF 3ª.1, 5ª y 11ª.2 LOPDGDD.

5.3 Las comunicaciones de datos

El RGPD, a diferencia de la LOPD, no prevé habilitaciones específicas para las comunicaciones de datos personales, sino que se les aplica el régimen general previsto para el resto de tratamientos.

Por lo tanto, cualquier comunicación de datos requiere alguna de las bases jurídicas mencionadas. Si, además, conlleva el tratamiento de categorías especiales de datos, también debe concurrir alguna de las excepciones previstas en el artículo 9.2 del RGPD.

Hay que tener en cuenta que, en el caso de las funciones públicas del colegio, aunque en principio no resulte aplicable la base jurídica consistente en la satisfacción de sus intereses legítimos, sí que puede habilitar la comunicación de datos a terceras personas fundamentada en los intereses legítimos de estas personas.

¿Es legítimo que los miembros de la junta o la asamblea del colegio accedan a las retribuciones de todos los trabajadores del colegio?

Los miembros de la junta o asamblea general de un colegio profesional pueden acceder a los datos de las retribuciones de los diferentes puestos de trabajo del colegio –sin necesidad de identificar, con carácter general, a las personas que ocupan los puestos-, en la medida que resulte necesario para ejercer las funciones que tenga atribuidas este órgano. Eso sin perjuicio de la posibilidad de acceder directamente a las retribuciones percibidas por los órganos de gobierno y directivos, de acuerdo con la normativa de transparencia que regula la publicidad activa.

¿Un colegio profesional puede comunicar a un medio de comunicación información sobre los complementos salariales de un cargo directivo del colegio?

Sí. De acuerdo con la legislación de transparencia, aplicable a las funciones públicas del colegio, hay que publicar de manera individualizada la información sobre todas las retribuciones percibidas por sus órganos de gobierno y cargos directivos. Además, es criterio reiterado tanto de esta Autoridad como de la Comisión de Garantía de Acceso a la Información Pública (GAIP) que respecto de otro personal que se pueda considerar de confianza o con altas responsabilidades, normalmente asociadas a un elevado nivel retributivo, también se pueda facilitar esta información.

¿Los empleados de correos y otras empresas de mensajería pueden pedir los datos identificativos del personal del servicio de atención al público de un colegio profesional, a efectos de hacerlas constar en los acuses de recibo de la documentación entregada?

Puede ser adecuado a la normativa de protección de datos indicar en el acuse de recibo los datos identificativos de la persona que se hace cargo de la recepción. Ahora bien, no hay que facilitarlas, en el caso de notificaciones de órganos administrativos y judiciales de documentación presentada en el registro general apta para ser registrada. En este caso, es suficiente hacer constar el sello del colegio.

Un colegio profesional ha publicado un anuncio en un diario oficial sobre una notificación infructuosa en un expediente disciplinario, que no incluye el nombre y apellidos, sino sólo el número del DNI. ¿Es correcto?

Sí. En estos casos, el anuncio que publica el colegio tiene que identificar a la persona afectada exclusivamente con el número completo del DNI o documento equivalente, puesto que la finalidad del anuncio no es dar publicidad general al expediente, sino sólo poder practicar una notificación por edictos. Únicamente si la persona afectada no dispone de estos documentos identificativos, hay que identificarla mediante el nombre y apellidos. En ningún caso hay que publicar el nombre y apellidos conjuntamente con el número completo del DNI o de otros documentos equivalentes.

Normativa aplicable: art. 4.2, 6 y 9 RGPD; DA 7ª y 10ª LOPDGDD; art. 3.1.b) y 9.1.b) LTC.

5.3.1 Acceso de terceros a datos personales de las personas colegiadas a través de la ventanilla única

La normativa que regula los colegios profesionales prevé que tienen que disponer de una ventanilla única en su página web, a través de la cual deben ofrecer información clara, inequívoca y gratuita sobre los aspectos siguientes:

- El acceso al **registro de colegiados**, que tiene que estar permanentemente actualizado y en el cual deben constar, al menos, los datos siguientes: nombre y apellidos del profesional colegiado, número de colegiación, títulos oficiales que posee, domicilio profesional y situación de habilitación profesional.
- El acceso al **registro de sociedades profesionales**, que debe tener el contenido descrito en el artículo 8 de la Ley 2/2007, de 15 de marzo, de sociedades profesionales, que incluye determinada información personal como la identificación de los socios profesionales y no profesionales (y en relación con los socios profesionales, el número de colegiado y el colegio profesional al que pertenecen); y la identificación de las personas que se encargan de la administración y la representación, con indicación de la condición de socio profesional o no de cada una de ellas.
- Las vías de reclamación y los recursos que se pueden interponer en caso de conflicto entre el consumidor o usuario y un colegiado o el colegio profesional.
- Los datos de las asociaciones u organizaciones de consumidores y usuarios a las cuales los destinatarios de los servicios profesionales pueden dirigirse para obtener asistencia.
- El contenido de los códigos deontológicos.

¿Se adecua al RGPD la posibilidad de que un ciudadano acceda a datos que figuran en el registro de colegiados a través de la página web del colegio profesional?

Sí, porque se trata de una comunicación de datos habilitada por la Ley 2/1974 y la Ley 7/2006, que obligan a dar acceso público al registro de colegiados a través de su página web (ventanilla única).

¿Qué información es necesario publicar en la ventanilla única o comunicar en caso de consulta, respecto de los colegiados no ejercientes (incluidos los casos de jubilación o invalidez) y los colegiados dados de baja o difuntos o de sus herederos?

El colegio puede publicar a través de la ventanilla única o comunicar a terceros la información siguiente, tanto de profesionales ejercientes como no ejercientes: nombre y apellidos, número de colegiación, titulación, datos de contacto profesional (domicilio profesional, teléfono, dirección de correo electrónico, etc.) y situación de habilitación profesional. En cambio, no se pueden divulgar datos de las personas colegiadas dadas de baja ni de las personas herederas de un colegiado difunto. Con respecto a los datos de colegiados difuntos, aunque en principio no tienen que figurar en la ventanilla única, hay que tener presente que no se les aplica la normativa de protección de datos personales.

La normativa de protección de datos no impide la publicación del domicilio personal del colegiado, cuando coincida con el domicilio profesional. Eso sin perjuicio del deber de informar previamente a los profesionales afectados y de la posibilidad de que estos se opongan a la divulgación de este dato, cuando su situación personal lo justifique.

¿Se puede informar a un tercero de la fecha en que un abogado colegiado causó baja del colegio o pasó a la situación de no ejerciente?

El dato relativo a la fecha concreta en que un abogado colegiado pasa a la situación de no ejerciente no forma parte de los datos incluidos en la normativa que regula la ventanilla única, ni su publicación está amparada por el artículo 19 de la LOPDGDD. No obstante, dado que pueden existir diferentes casos en los que esta fecha sea relevante, el colegio puede facilitarla a un tercero siempre que se dé alguna de las condiciones de licitud del tratamiento que regula el RGPD (consentimiento, interés legítimo, etc.).

¿El motivo de la situación de inactividad de una persona colegiada puede formar parte del listado de profesionales? ¿Puede constar el período de tiempo de inactividad?

No. Aunque esta lista puede recoger la situación de no ejerciente o de inactividad temporal, no tiene que recoger los motivos a los cuales obedece esta situación, ni el período que la persona colegiada pueda permanecer en ella. La Ley 2/1974 recoge la obligación de ofrecer mediante la ventanilla única el dato de la situación de habilitación profesional, es decir, ejerciente o no ejerciente o inactividad temporal, pero no recoge la obligación de informar sobre una posible inhabilitación.

¿El listado de profesionales que se publica en la ventanilla única puede considerarse una fuente accesible al público?

Actualmente, la normativa de protección de datos no contiene una definición sobre qué hay que entender como fuente accesible al público, ni establece ningún régimen específico con respecto al tratamiento de los datos que pueden contener. Se puede considerar fuente de acceso público cualquier conjunto de información de libre acceso para la ciudadanía.

¿El colegio puede facilitar a un colegiado un listado de las direcciones electrónicas del resto de colegiados que se dedican a una especialidad?

Aunque el dato relativo a la especialidad no figura expresamente entre los datos del registro de colegiados que la Ley sobre Colegios Profesionales habilita a publicar a través de la ventanilla única (art. 40.bis de la Ley 7/2006), hay que tener en cuenta que la información relativa a la especialidad puede estar estrechamente relacionada con las titulaciones o con la situación de habilitación profesional. Por lo tanto, hay que admitir la publicación o la comunicación de este dato a cualquier persona, ya que se trata de un aspecto que puede resultar necesario para garantizar mejor los derechos de las personas consumidoras y usuarias.

¿Cuáles son los datos de las sociedades profesionales inscritas que hay que publicar en la ventanilla única?

El colegio tiene que publicar la información que prevé el artículo 8 de la Ley 2/2007, de 15 de marzo, de sociedades profesionales, que incluye determinada información personal como la identificación de los socios profesionales (número de colegiado y colegio profesional al que pertenece) y no profesionales, y la identificación de las personas que se encargan de la administración y la representación, con indicación de la condición de socio profesional o no de cada una de ellas.

Respecto a las personas encargadas de la administración y representación de estas sociedades, se puede dar acceso a sus datos identificativos. En ambos casos se pueden publicar los datos de contacto profesional.

¿Se pueden facilitar los datos de un colegiado a un tercero, cuando las solicita por teléfono o por correo electrónico?

Sí. Si la comunicación se limita a los datos incluidos en la lista de profesionales que tiene que publicar, hay que considerarla vinculada directamente con el cumplimiento de una de las funciones públicas del colegio, prevista en la Ley 7/2006. Para comunicar otros datos no incluidos en la lista mencionada (por ejemplo, DNI, datos bancarios, domicilio particular, etc.), hay que disponer de alguna otra base jurídica.

¿Un colegio puede comunicar datos de los colegiados a la empresa aseguradora con la que tiene contratada el seguro colectivo de responsabilidad civil profesional?

Sí, si el colegio ha establecido un seguro colectivo de este tipo, la incorporación del colegiado en el colegio conlleva que pase a tener la condición de asegurado. La comunicación de datos sería necesaria para desarrollar esta relación jurídica. Eso, sin perjuicio de que el colegio tiene que informar a los colegiados sobre esta comunicación.

¿Se puede divulgar la identidad de las personas colegiadas que impulsan la inclusión de un punto del orden del día de la asamblea del colegio?

Hay que poder verificar la identidad y la condición de colegiadas de las personas promotoras de la iniciativa, como requisito para admitirla. Además, el resto de personas colegiadas están legitimadas para consultar la documentación relativa a la convocatoria de la asamblea. Por lo tanto, la comunicación al resto de personas colegiadas de la proposición de incluir un nuevo punto del orden del día, identificando a las personas promotoras, es conforme a la normativa de protección de datos personales.

Normativa aplicable: art. 10 Ley 2/1974; 40 bis Ley 7/2006; Recomendación 1/2008.

5.3.2 Acceso de los candidatos en un proceso electoral a los datos de colegiados

El acceso de los candidatos al censo electoral se puede considerar amparado en la existencia de un interés legítimo.

Por otra parte, respecto al régimen de acceso a los datos que contiene el censo electoral del colegio, se puede considerar aplicable la Ley Orgánica del Régimen Electoral General (LOREG) como norma supletoria. En este sentido, el artículo 41.5 de la LOREG habilitaría al colegio para proporcionar a los candidatos la copia del censo al día siguiente de que se proclamen como candidatos, sin necesidad de obtener el consentimiento previo de las personas afectadas, ya que la cesión está habilitada por la previsión de esta obligación en una norma con rango de ley.

Hay que excluir de esta lista a las personas que han ejercido su derecho de oposición alegando motivos fundamentados en su situación personal que justifiquen la exclusión, o la no revelación de algunos de sus datos (por ejemplo, su dirección postal). En este último caso, el envío de información electoral se puede hacer a una dirección electrónica o un apartado de correos que haya designado la persona afectada.

En cualquier caso, desde el punto de vista del derecho a la protección de datos puede ser conveniente que, en el momento de regular el procedimiento electoral en sus estatutos, los colegios valoren otras posibilidades diferentes del envío a la dirección postal de los colegiados, como por ejemplo el envío a una dirección electrónica designada por el colegiado, el envío postal conjunto hecho por el mismo colegio, etc.

¿Se puede entregar un listado de las personas colegiadas, con indicación de sus datos de contacto, a una persona colegiada interesada en contribuir a las elecciones a la junta de gobierno del colegio?

La entrega de un listado de los colegiados (nombre, apellidos y dirección de correo electrónico) a una persona colegiada, proclamada candidata se puede considerar enmarcado en la satisfacción de intereses legítimos y, por lo tanto, un tratamiento

amparado en la base jurídica del artículo 6.1.f) del RGPD. La información mencionada sólo se puede utilizar para la finalidad específica de facilitar la comunicación entre las personas candidatas y el resto de personas colegiadas durante el período de campaña electoral.

La normativa de protección de datos no establece previsiones específicas en relación con la forma concreta de entregar los datos personales.

Normativa aplicable: art. 6.1.c) RGPD; 41.5 LOREG.

5.3.3 Comunicación de sanciones disciplinarias, inhabilitaciones e incompatibilidades

A los efectos que establece el artículo 3.3 de la Ley 2/1974, los colegios pueden comunicar las sanciones disciplinarias impuestas a sus colegiados al resto de los colegios territoriales de la profesión de que se trate. Esta habilitación afecta sólo a la información necesaria para que la resolución sancionadora pueda desplegar sus efectos en todo el territorio.

Hay que tener en cuenta que la ventanilla única puede reflejar las consecuencias de la inhabilitación (el colegiado no aparecerá como ejerciente), pero sin hacer referencia a la sanción de inhabilitación.

¿En qué casos los colegios están habilitados por la ley para comunicar información relativa a la comisión de infracciones administrativas y a la imposición de sanciones?

La comunicación de información sobre la comisión de infracciones administrativas o la imposición de sanciones está habilitada por ley cuando se comunican las sanciones disciplinarias que implican inhabilitación o separación profesional al consejo de colegios, para que las traslade al resto de colegios y a los órganos judiciales (art. 6.1.e y 6.4 RGPD y art. 3.3 de la Ley 2/1974).

En el resto de supuestos no hay, con carácter general, una habilitación legal que permita dar publicidad a los expedientes o las resoluciones sancionadoras ni publicar las sanciones impuestas. Eso, sin perjuicio de que cuando se haya impuesto una sanción de inhabilitación o de separación el colegiado afectado deba excluirse de la lista de profesionales del colegio, mientras duren los efectos de la sanción.

¿Un colegio profesional puede comunicar a una universidad, con la finalidad de controlar el cumplimiento del régimen de incompatibilidades, una lista de los proyectos visados respecto de determinados profesionales que también tienen la condición de profesores de la universidad mencionada?

La universidad puede acceder a los datos personales incluidos en la ventanilla única.

Por otra parte, en el marco de un procedimiento por incumplimiento de la normativa de incompatibilidades, también se puede comunicar a la universidad el dato consistente en si profesores con dedicación a tiempo completo han solicitado el

visado de ciertos trabajos profesionales, sin necesidad de requerir el consentimiento previo de estos profesores.

¿Un colegio profesional puede publicar la resolución de baja forzosa de un colegiado por impago, en el tablón de anuncios o en un diario oficial?

No. Cuando las resoluciones adoptadas no se han podido notificar personalmente a los colegiados afectados, el colegio está habilitado legalmente para notificarlas por medio de un anuncio en el boletín oficial, pero eso no incluye la publicación de la resolución. El anuncio debe identificar a la persona afectada exclusivamente con su número de DNI y tiene que limitarse a incluir la información necesaria para que la persona afectada pueda recoger la notificación.

Normativa aplicable: art. 6.1.c) RGPD; 3.3 y 10.2.a) Ley 2/1974; DA 7ª LOPDGDD.

5.3.4 Comunicaciones de datos a administraciones públicas, a otros colegios y a los consejos de colegios

Los colegios profesionales de ámbito territorial deben facilitar a los consejos generales o superiores, y si procede a los consejos autonómicos de colegios, la información relativa a las altas, bajas y cualquier otra modificación que afecte a los registros de colegiados y de sociedades profesionales, para que tomen conocimiento y lo anoten en sus registros centrales de colegiados y de sociedades profesionales.

Aparte de eso, en otros supuestos, los colegios profesionales pueden tener que comunicar datos a otras administraciones públicas. Será necesaria alguna de las bases jurídicas del artículo 6 del RGPD. En cualquier caso, si no se dispone del consentimiento o de una ley que lo prevea expresamente, la comunicación sólo se puede realizar para una actividad que sea compatible.

¿Un colegio de abogados puede comunicar al consejo de colegios la lista de colegiados inscritos en el turno de oficio y asistencia al detenido?

El colegio profesional puede comunicar este listado al Consejo de la Abogacía Catalana, sin requerir el consentimiento previo a los profesionales afectados, si es necesario para controlar que se cumple el régimen de incompatibilidades previsto para la inscripción al servicio del turno de oficio de un determinado colegio profesional. Esta comunicación encuentra legitimación en el artículo 6.1.e) y 6.4 del RGPD, al tratarse de una cesión de datos entre corporaciones públicas para ejercer una competencia pública que versa sobre una misma materia, como es la de regular y organizar los servicios de asistencia letrada y defensa y representación gratuita, la cual incluye velar por el correcto funcionamiento de este servicio.

Eso no excluye la obligación de cumplir el deber de información. De acuerdo con lo que dispone el artículo 14 del RGPD, el Consejo de los Colegios tiene que informar a los profesionales de manera expresa, precisa e inequívoca, en un plazo razonable y

como máximo de un mes desde la comunicación, a menos que el colegio profesional ya los haya informado anteriormente.

¿Hay que pedir el consentimiento para ceder los datos de que dispone la demarcación territorial catalana del colegio profesional de ámbito estatal para constituir un colegio profesional catalán independiente?

Los datos se pueden ceder sin el consentimiento de los afectados, en la medida que de las previsiones de la Ley 7/2006, de 31 de mayo, del ejercicio de profesiones tituladas y de los colegios profesionales, se desprende que hay habilitación legal suficiente para realizar la comunicación (artículo 6.1.e) y 6.4). La cesión tiene que comprender sólo los datos personales de las personas colegiadas con domicilio profesional único o principal en Cataluña, que sean adecuados, pertinentes y no excesivos para que puedan colegiarse en el colegio de Cataluña.

El nuevo colegio será el nuevo responsable del tratamiento y tendrá que cumplir el deber de información a los afectados en los términos establecidos al artículo 14 del RGPD, así como el resto de principios y obligaciones previstas en la normativa de protección de datos personales.

¿Un colegio de abogados puede comunicar información a la Administración tributaria sobre los informes elaborados en relación con minutas presentadas por abogados colegiados?

La comunicación generalizada de información sobre este tipo de informes –que incluya la identificación de los abogados correspondientes- a la Administración tributaria no resulta justificada al amparo del artículo 94.1 de la LGT, dada la falta de trascendencia tributaria de estos informes, ya que son sólo estimaciones provisionales sobre los honorarios, y que no hay una disposición general que prevea este requerimiento generalizado de información.

¿Un colegio puede comunicar datos de salud de las personas colegiadas a una administración pública, para realizar un estudio estadístico?

Si un colegio dispone de datos de salud de sus colegiados y una administración pública los requiere para realizar un estudio estadístico sobre morbilidad de determinados colectivos profesionales, en ausencia del consentimiento de las personas afectadas el colegio sólo puede comunicar estos datos previa anonimización.

¿Un colegio puede acceder a información de que disponen las administraciones públicas, para controlar el cumplimiento del deber de colegiación de determinados profesionales?

Sí, dado que el control de la colegiación obligatoria forma parte de las funciones atribuidas a los colegios profesionales.

¿Un colegio profesional puede comunicar a un juzgado el dato relativo al número de identificación fiscal de un colegiado?

Si un juez lo requiere para ejercer las funciones que tiene atribuidas, esta comunicación se adecua a la normativa de protección de datos, ya que tiene la habilitación legal en el RGPD y en la LOPJ.

Normativa aplicable: art. 6.1 letras c) y e) RGPD; art. 25 LOPDGDD; 10.4 Ley 2/1974; Ley 1/1996.

5.3.5 Comunicación de datos a cuerpos policiales

Respecto a las comunicaciones de datos a los cuerpos policiales, hay que tener en cuenta que la Ley Orgánica 7/2021 dispone la obligación de cualquier persona física o jurídica de proporcionar a las autoridades competentes los datos, los informes y los justificantes necesarios que les soliciten, de manera motivada, concreta y específica, en los supuestos siguientes:

- Para la investigación y el enjuiciamiento de infracciones penales o para la ejecución de penas por parte de las autoridades judiciales, el ministerio fiscal o la policía judicial.
  De las solicitudes de información realizadas por la policía judicial, se tiene que dar cuenta en todo caso a la autoridad judicial y fiscal. La comunicación de datos que lleven a cabo la Administración tributaria, la Inspección de Trabajo y la Administración de la Seguridad Social debe hacerse de acuerdo con su legislación específica.
- Para la prevención, la detección y la investigación de infracciones penales por las autoridades competentes.
- Para la prevención y la protección enfrente de un peligro real y grave para la seguridad pública por las autoridades competentes.

Estas determinaciones no eximen de obtener la autorización judicial pertinente, cuando sea exigible.

Incumplir este deber de colaboración, o facilitar información a las personas afectadas por estas comunicaciones, se tipifica como infracción en diferentes preceptos de la Ley Orgánica (art. 58.j y 59.j).

Normativa aplicable: art. 7 Ley Orgánica 7/2021.

5.4 Disposiciones aplicables a tratamientos específicos

5.4.1 Tratamiento de datos relativos a infracciones y sanciones administrativas

El RGPD no regula específicamente el tratamiento de datos relativos a infracciones y sanciones administrativas. Ahora bien, la LOPDGDD sí que establece determinadas condiciones específicas para tratar estos datos, de los cuales formarían parte, por ejemplo, los datos relativos a las infracciones disciplinarias impuestas al amparo de la normativa que regula los colegios profesionales. En concreto, la LOPDGDD permite que los puedan tratar los órganos competentes para instruir el procedimiento sancionador, para declarar las infracciones o imponer las sanciones, siempre que el tratamiento se limite a los datos estrictamente necesarios para esta finalidad.

Fuera de este supuesto, sólo se pueden tratar si:

- Se cuenta con el consentimiento expreso de la persona afectada.
- Lo autoriza una norma con rango de ley, que debe regular, si procede, garantías adicionales para los derechos y las libertades de las personas afectadas.
- El tratamiento lo llevan a cabo abogados o procuradores a partir de la información facilitada por sus clientes para ejercer sus funciones.

En cualquier caso, este tipo de datos quedan excluidos del derecho de acceso a la información pública regulado por la legislación de transparencia, a menos que las personas hayan consentido, que lo prevea una ley o que la misma persona afectada las haya hecho manifiestamente públicas.

Normativa aplicable: art. 27 LOPDGDD; art. 15.1 LT; art. 23 LTC.

5.4.2 Tratamiento de datos del personal de los colegios profesionales

5.4.2.1 Datos de contacto profesional del personal del colegio

Los colegios profesionales responsables o encargados del tratamiento pueden publicar los datos profesionales de contacto y, si procede, los relativos a la función o el lugar que ejerzan las personas físicas que prestan servicios, cuando se derive de una obligación legal o sea necesario para ejercer sus funciones.

Requisitos:

- El tratamiento tiene que referirse únicamente a los datos necesarios para su localización profesional.
- La finalidad del tratamiento debe ser únicamente mantener relaciones de cualquier índole con el colegio profesional.

Normativa aplicable: art.19 LOPDGDD.

5.4.2.2 Videovigilancia en el ámbito laboral

Los colegios profesionales pueden tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para ejercer las funciones de control de sus trabajadores, siempre que se ejerzan dentro de su marco legal y con los límites inherentes a este.

Para valorar la proporcionalidad de la instalación del sistema de videovigilancia hay que tener en cuenta:

- Si el sistema de videovigilancia es apto para conseguir la finalidad perseguida.
- Si no existen otras medidas menos intrusivas para conseguir la finalidad con la misma eficacia.
- Si es una medida equilibrada, es decir, si ofrece más beneficios para el interés general que perjuicios.

El uso de sistemas similares para grabar voces en el puesto de trabajo se admite únicamente cuando concurren riesgos relevantes para la seguridad de las instalaciones, los bienes y las personas, derivados de la actividad que se lleva a cabo en el centro de trabajo.

En cualquier caso, el uso de estos sistemas está sometido a determinados límites y garantías:

- Intervención mínima, es decir, los controles deben tener como objetivo inspeccionar la ejecución de las obligaciones laborales, sin exceder de cuestiones vinculadas a su desarrollo.
- El respeto a la dignidad de la persona trabajadora. En ningún caso se admite la instalación de sistemas de grabación de sonidos ni de videovigilancia en vestuarios o lavabos, ni en lugares destinados al descanso o esparcimiento de las personas trabajadoras, como comedores o lugares análogos.
- Antes de iniciar la captación, el colegio tiene que informar a los trabajadores, y si procede a sus representantes, de la existencia de estos dispositivos, de manera expresa, clara e inequívoca, de acuerdo con lo que se establece en el apartado 5.4.4 de esta guía.
  Si se han captado trabajadores en la comisión flagrante de un acto ilícito, se entiende cumplido el deber de informar cuando esté al menos el dispositivo informativo en un lugar lo bastante visible que informe de la existencia del tratamiento, de la identidad del responsable y de la posibilidad de ejercer los derechos que prevén los artículos 15 a 22 del RGPD.
- Los sistemas de videovigilancia que capten imágenes o voces, con independencia de que se graben o no, se tienen que inscribir en el registro de actividades de tratamiento. El sistema de videovigilancia puede estar formado por una cámara o por

varias cámaras en una misma instalación o en varias, siempre que obedezcan a una misma finalidad y el tratamiento tenga unas características equiparables.

Cuando un colegio profesional implante un sistema de videovigilancia que implique el acceso de una empresa de seguridad privada a las imágenes o voces que se capten, esta empresa tiene la consideración de encargado del tratamiento.

La supresión de los datos de estos sistemas de grabación debe llevarse a cabo en el plazo máximo de un mes desde que se captaron, excepto cuando haya que conservarlos para acreditar que se han cometido actos que atentan contra la integridad de personas, bienes o instalaciones. En este caso, las imágenes deben ponerse a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tiene conocimiento de la existencia de la grabación.

La obligación de bloqueo que prevé el articulo 32 de la LOPDGDD no es aplicable a estos tratamientos.

Sobre esta cuestión, hay que tener en cuenta también lo que se expone en el apartado 5.4.4 de esta guía y en especial la Instrucción 1/2009 de esta Autoridad, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

Un colegio profesional quiere instalar videocámaras en la sede colegial para finalidades de seguridad y de control horario con fines laborales. ¿Qué hay que tener en cuenta?

Hay que tener en cuenta si la instalación de cada cámara responde a una u otra finalidad, o a las dos, y analizar en consecuencia si se ajusta a la normativa y en especial a la Instrucción 1/2009. Sólo pueden acceder a las imágenes las personas autorizadas por razón de sus funciones. Hay que tener especialmente en cuenta el principio de proporcionalidad.

Con respecto a las cámaras con finalidades de control laboral, aparte de analizar si hay mecanismos de control horario y de presencia alternativos y menos lesivos para los derechos de las personas afectadas para determinar la proporcionalidad, hay que informar a los trabajadores y sus representantes de que se han instalado.

¿Cuál tiene que ser el plazo de conservación de las imágenes de las cámaras con la finalidad de control laboral?

En relación con los tratamientos de videovigilancia, la LOPDGDD prevé el plazo de conservación de un mes como máximo. Eso no quiere decir que necesariamente se deba agotar este plazo. Por aplicación del principio de limitación del plazo de conservación, hay que suprimir las imágenes lo antes posible, si no hay circunstancias que justifiquen la conservación.

Normativa aplicable: art. 22 y 89 LOPDGDD; art. 20 y 20.bis TE.

5.4.2.3 Uso de dispositivos digitales

Las personas trabajadoras tienen derecho a la protección de su intimidad en el uso de los dispositivos digitales, como ordenadores, tabletas, *smartphones* o cuentas de correo que el colegio ponga a su disposición.

El colegio sólo puede acceder a los contenidos derivados del uso de medios digitales facilitados a las personas trabajadoras para las finalidades siguientes:

- Controlar el cumplimiento de las obligaciones laborales.
- Garantizar la continuidad de los servicios.
- Garantizar la integridad de los dispositivos mencionados.

El uso de dispositivos digitales requiere:

- Que el colegio establezca los criterios de utilización, respetando los estándares mínimos de protección de la intimidad de los trabajadores de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente.
  Los representantes de las personas trabajadoras tienen que poder participar en la elaboración de estos criterios.
- Que se informe a las personas trabajadoras de los criterios establecidos.

El acceso del colegio profesional al contenido de dispositivos digitales respecto de los cuales haya admitido el uso con finalidades privadas requiere:

- Que se hayan especificado los usos autorizados de forma precisa.
- Que se establezcan garantías para preservar la intimidad de las personas trabajadoras (por ejemplo, presencia de la persona afectada, si es posible, o en su defecto, de un representante de los trabajadores; levantar un acta; garantizar el no acceso a la información privada que pueda constar; etc.).

Sobre esta cuestión se recomienda consultar la Recomendación 1/2013, de esta Autoridad, sobre el uso del correo electrónico en el ámbito laboral.

¿Un colegio profesional puede controlar los ordenadores asignados a sus trabajadores, con la finalidad de verificar el uso?

Sí. Si el tratamiento se lleva a cabo durante la prestación del servicio y para asegurar el normal funcionamiento, el colegio no necesitaría disponer del consentimiento previo de las personas afectadas. En cualquier caso, conviene tener aprobadas normas internas sobre el uso de las TIC, que sean conocidas por los trabajadores, y llevar a cabo la intervención de acuerdo con estas normas y con el principio de proporcionalidad.

Normativa aplicable: art. 87 LOPDGDD; art. 20 y 20.bis TE.

5.4.3 Tratamiento de datos de contacto de personas al servicio de personas jurídicas, de empresarios individuales y de profesionales liberales

Los colegios profesionales pueden tratar los datos necesarios para la localización profesional de los profesionales liberales y empresarios individuales, cuando se refieran únicamente a esta condición y no se traten para establecer una relación como personas físicas, siempre que se derive de una obligación legal o sea necesario para ejercer sus funciones públicas.

También pueden tratar los datos de contacto y, si procede, los relativos a la función o el lugar que ejercen, de las personas físicas que prestan servicios en una persona jurídica, cuando:

- Se traten únicamente los datos necesarios para su localización profesional.
- La finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que la persona afectada preste sus servicios.
- Se derive de una obligación legal o sea necesario para ejercer sus funciones públicas.

¿Un colegio profesional puede utilizar datos de contacto profesional de trabajadores de empresas, de personal de la administración o de profesionales liberales recogidos de las páginas web de estas organizaciones, para establecer contacto profesional?

Sí. Siempre que sea para establecer contacto profesional.

Normativa aplicable: art. 19 LOPDGDD.

5.4.4 Tratamiento con finalidades de videovigilancia

Los colegios profesionales pueden captar imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

No obstante, con carácter general, los colegios profesionales no pueden captar imágenes de la vía pública con estos sistemas, a menos que sea imprescindible para la finalidad de preservar la seguridad de las personas y bienes, y de sus instalaciones.

Los colegios profesionales tienen que informar de la existencia de las cámaras, colocando un cartel informativo en un lugar lo bastante visible con el contenido mínimo siguiente:

- La existencia del tratamiento.
- La identidad del responsable.
- La posibilidad de ejercer los derechos que prevén los artículos 15 a 22 del RGPD.
- El lugar donde las personas afectadas pueden obtener el resto de información sobre el tratamiento que requiere el RGPD. Debe incluirse un código de conexión o una dirección de internet para obtener esta información.

Hay que tener en cuenta que la ubicación de los carteles informativos tiene que permitir a las personas afectadas prever cuáles son las áreas vigiladas. Así, para las cámaras de videovigilancia en edificios o instalaciones, hay que colocar un cartel informativo en cada uno de los accesos al área videovigilada. Si están divididos por plantas con diferentes responsables o con finalidades diferentes, además, hay que colocar otro cartel informativo en cada una de las plantas donde haya cámaras, ubicado en un espacio de acceso principal al área o zona videovigilada.

Los datos deben suprimirse en el plazo máximo de un mes desde su captación. Cuando haya que conservarlos para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, las imágenes deben ponerse a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tiene conocimiento de la existencia de la grabación.

La obligación de bloqueo no es aplicable a estos tratamientos.

Sobre esta cuestión hay que tener en cuenta la Instrucción 1/2009 de esta Autoridad, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

¿Se pueden instalar cámaras de videovigilancia en la sede del colegio con fines de seguridad?

Sí, dado que, siempre que se respeten el resto de principios y garantías de la normativa de protección de datos, la implantación de este tipo de sistemas de videovigilancia en sus instalaciones se puede considerar incluida en el cumplimiento de la misión en interés público que tienen encomendada los colegios profesionales.

¿Cuánto tiempo pueden conservarse las imágenes obtenidas a través de un sistema de videovigilancia?

Cuando no pueda alcanzarse la finalidad perseguida sin almacenar las imágenes, el período de conservación no debe ser superior al necesario para cumplir la finalidad de vigilancia para la que se han recogido o grabado. Con carácter general, no puede excederse el plazo de un mes para suprimirlas.

¿Cómo se aplican las medidas de seguridad a los tratamientos de datos mediante sistemas de videovigilancia?

Las medidas de seguridad tienen que determinarse caso por caso, de acuerdo con el análisis de riesgos realizado. Las medidas de seguridad deben ser apropiadas para

garantizar la confidencialidad, la integridad y la disponibilidad de los datos. En este sentido, conviene tener en cuenta las previsiones específicas en materia de videovigilancia que contiene la Instrucción 1/2009.

¿En qué casos hay que hacer copias de seguridad de los tratamientos de videovigilancia?

De acuerdo con la Instrucción 1/2009, si los datos se guardan por un período superior a una semana, hay que hacer copias de seguridad semanalmente.

Normativa aplicable: art. 22 LOPDGDD; Instrucción 1/2009.

5.4.5 Sistemas internos de denuncias

Los colegios profesionales pueden crear sistemas de información a través de los cuales se les pueda comunicar la comisión, en el colegio o en la actuación de contratistas del colegio, de actos o conductas que puedan ser contrarios a la normativa general o sectorial aplicable. Estas denuncias pueden ser anónimas.

En todo caso, hay que adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos de las personas afectadas por la información suministrada, especialmente la de la persona que ha comunicado los hechos a la entidad y se ha identificado.

Hay que informar a los empleados y a los contratistas sobre la existencia de estos sistemas de información.

Sólo pueden acceder a los datos contenidos en estos sistemas:

- Las personas que ejercen las funciones de control interno y de cumplimiento, incluidos los encargados del tratamiento que se designen eventualmente.
- El personal con funciones de gestión y control de recursos humanos, únicamente cuando pueda proceder la adopción de medidas disciplinarias respecto de una persona trabajadora.
- Otras personas, cuando sea necesario para adoptar medidas disciplinarias o para tramitar los procedimientos judiciales.

Los datos de quien ha hecho la comunicación, los de los trabajadores y los de terceros deben conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, los datos deben suprimirse del sistema de denuncias una vez transcurridos tres meses desde que se introdujeron. Sin embargo, el órgano al que corresponde investigar los hechos denunciados los puede continuar tratando con esta finalidad.

Las denuncias que no se hayan cursado sólo pueden constar en el sistema de manera anonimizada.

No es aplicable la obligación de bloqueo.

¿Un trabajador de una empresa que presta servicios al colegio puede utilizar el sistema de información de denuncias internas para comunicar al colegio deficiencias en la gestión del servicio?

Sí. El sistema de denuncias internas del colegio también permite informar de conductas o actos en la actuación de los contratistas que puedan ser contrarios a la normativa general o sectorial aplicable.

Normativa aplicable: art. 24 LOPDGDD.

5.4.6 Tratamiento de datos con finalidades estadísticas

Se entiende por tratamiento con finalidades estadísticas cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos de acuerdo con la normativa que regula la estadística oficial. Estos resultados se pueden utilizar con diferentes finalidades, incluida la investigación científica.

El tratamiento de datos personales con finalidades estadísticas debe someterse a lo que dispone su legislación específica, en especial con respecto a la regulación del secreto estadístico, así como en el RGPD y la LOPDGDD.

El RGPD prevé que el tratamiento con finalidad estadística se puede considerar compatible con la finalidad inicial del tratamiento, siempre que se adopten garantías adecuadas para los derechos y libertades de las personas afectadas. Si se tratan categorías especiales de datos, es necesario que el tratamiento con finalidades estadísticas esté previsto expresamente en una norma con rango de ley, que sea proporcional al objetivo perseguido y que prevea garantías adecuadas.

La comunicación de los datos a los órganos competentes en materia estadística sólo se entiende habilitada para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, cuando:

- La estadística para la cual se requiere la información es exigida por una norma de derecho de la Unión.
- Está incluida en los instrumentos de programación estadística previstos legalmente.

El tratamiento con finalidades estadísticas requiere:

- Que los datos personales tratados sean adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las cuales se tratan.
- Que se garanticen los derechos y las libertades de las personas afectadas, adoptando las medidas técnicas y organizativas adecuadas. Estas medidas pueden incluir la seudonimitzación o la anonimización, siempre que sea posible.
- Que, aparte del deber de información previsto en el artículo 13 del RGPD, se informe a la persona de la cual se solicitan los datos de lo siguiente:
  - El carácter y la finalidad de la estadística.
  - El carácter obligatorio o facultativo de las respuestas.
  - La consecuencia de la falta de respuesta.
  - Las garantías para preservar el anonimato (secreto estadístico).
- Las categorías especiales de datos y los datos personales relativos a condenas e infracciones penales son de aportación estrictamente voluntaria y sólo se pueden recoger con el consentimiento previo expreso de las personas afectadas.
- El resultado del tratamiento con finalidades estadísticas no puede comportar la difusión de datos personales, sino de datos agregados que no deben permitir identificar a personas físicas. Ni el resultado ni los datos personales que se utilizan con esta finalidad pueden utilizarse para respaldar medidas o decisiones relativas a personas físicas concretas.
- Se pueden denegar las solicitudes de ejercicio de los derechos de las personas afectadas previstos en el RGPD de los datos amparados por las garantías del secreto estadístico.

Normativa aplicable: considerando 162 y art. 5.1.*b)*, 9.2.*j)* y 89 RGPD; art. 25 LOPDGDD; LEC.

6. Obligaciones del responsable del tratamiento antes de iniciar el tratamiento

Antes de emprender cualquier actuación que implique el tratamiento de datos personales, el colegio responsable del tratamiento tiene que llevar a cabo una serie de actuaciones:

1. Hacer un **análisis** del "ciclo de vida" o recorrido de los datos a lo largo de su tratamiento, con el fin de identificar:

   - Si es necesario un nuevo tratamiento.
   - Qué datos personales hay que recoger y para qué finalidad.
   - Cómo se recogerán (formularios en papel, electrónicamente, telefónicamente, etc.).
   - Quién los tratará (áreas, departamentos, personas usuarias, etc.).
   - Cómo circularán dentro de la entidad (en soporte papel, telemáticamente, etc.).

- A quién se cederán o qué transferencias internacionales se harán y cómo se realizará.
- Cómo se conservarán y, si procede, cómo y cuándo se destruirán.

2. Diseñar el trámite o servicio teniendo en cuenta el derecho a la protección de datos: **protección de datos desde el diseño** y **protección de datos por defecto**.

3. Hacer un análisis de riesgos.

4. Realizar, si procede, una evaluación de impacto y una consulta previa.

5. Incorporar la actividad de tratamiento al **registro** y al **inventario de actividades del tratamiento**.

6.1 La proporcionalidad del tratamiento; el principio de minimización

De acuerdo con el principio de minimización, manifestación del principio de proporcionalidad en el ámbito de la protección de datos, los datos personales tienen que ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las cuales se tratan.

Este principio conlleva:

- Evitar tratamientos generalizados, excesivamente amplios, indiscriminados o genéricos.
- No tratar datos personales cuando no sea necesario para alcanzar una determinada finalidad.
- Cuando haya que tratar datos personales, utilizar sólo los mínimos e indispensables.
- Utilizar, cuando sea posible, el mecanismo de la seudonimización. Este mecanismo permite que puedan tratarlos trabajadores del colegio profesional o de un encargado del tratamiento y, si procede, terceras personas sin que tengan acceso a los datos identificativos. A pesar de seguir siendo datos personales, la seudonimización permite minimizar los riesgos inherentes a cualquier tratamiento de datos personales.

Normativa aplicable: art. 5.1.*c)* RGPD.

¿El colegio puede recoger cualquier tipo de información sobre los colegiados?

De acuerdo con el principio de minimización de datos, el colegio sólo puede recoger y tratar los datos que sean adecuados, pertinentes y limitados a lo necesario en relación con el ámbito y las finalidades relacionadas con su actividad.

¿La información de un colegiado se puede limitar, a petición suya, a un simple apartado de correos?

No. De acuerdo con la normativa reguladora de las funciones de los colegios profesionales, los colegios tienen que tratar otros datos necesarios para mantener la relación jurídica establecida entre el colegiado y el colegio profesional.

6.2 La protección de datos desde el diseño y por defecto

La protección de datos desde el diseño implica que el responsable, tanto en el momento de determinar los medios de tratamiento como en el momento del tratamiento mismo, atendiendo el estado de la técnica, el coste de la aplicación, la naturaleza, el ámbito, el contexto y las finalidades del tratamiento, así como los riesgos que entraña el tratamiento para los derechos y las libertades de las personas, tiene que hacer lo siguiente:

- Implantar las medidas técnicas y organizativas adecuadas para aplicar de forma efectiva los principios de protección de datos (como la seudonimización).
- Integrar las garantías necesarias en el tratamiento, para proteger los derechos de las personas afectadas.

La protección de datos por defecto obliga al responsable del tratamiento a aplicar las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, el tratamiento afecta de la menor forma posible a las personas afectadas. Así, por ejemplo, implica que:

- Únicamente se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento.
- El alcance del tratamiento es sólo el estrictamente necesario para conseguir la finalidad perseguida.
- Los datos sólo se conservan durante el plazo necesario para alcanzar la finalidad perseguida.
- Los datos personales no son accesibles a un número indeterminado de personas físicas, sin la intervención de la persona afectada.

¿Qué implican la protección de datos desde el diseño y la protección de datos por defecto, en la puesta en marcha de una app para ofrecer un nuevo servicio?

Siguiendo estos principios, en el momento de diseñar la aplicación el colegio tendría que analizar todas las implicaciones que puede comportar su puesta en marcha para la protección de datos de las personas afectadas: necesidad o no de tratar datos personales, datos concretos que se recogen, plazo de conservación, medidas de seguridad, ejercicio de derechos dentro de la aplicación, etc., e incorporar medidas para minimizar los riesgos que se generen (protección de datos desde el diseño).

Al mismo tiempo, tendría que velar, por ejemplo, para que la comunicación de datos a terceras personas requiera una acción positiva de la persona usuaria o para que la

geolocalización de las personas usuarias sólo permanezca activa cuando la app esté en uso, y que eso requiera una acción positiva de la persona usuaria (protección de datos por defecto).

Normativa aplicable: considerando 78 y art. 25 RGPD.

6.3 El análisis de riesgos

El análisis de riesgos es el instrumento a partir del cual el responsable del tratamiento determina las medidas técnicas y organizativas necesarias para establecer un nivel de seguridad adecuado al riesgo.

Para hacer un análisis de riesgos es necesario:

- Identificar las amenazas y los riesgos: posible fuga de información, suplantación de identidades, errores técnicos que provoquen una duplicación de registros con información contradictoria, destrucción de la información por causas ambientales, cortes de suministro eléctrico, etc.
- Evaluar el riesgo: si hay alguna probabilidad de que la amenaza se produzca y qué impacto tendría (probabilidad y gravedad del riesgo).
- Tratar el riesgo: qué medidas se pueden aplicar para reducir la probabilidad de que la amenaza se produzca y el impacto que causaría en la persona afectada.

El análisis de riesgos debe realizarse antes del inicio del tratamiento y tiene que revisarse periódicamente y siempre que se produzca algún cambio sustancial en el tratamiento.

Para identificar y evaluar los riesgos, hay que tener especialmente en cuenta si el tratamiento puede comportar alguna de estas situaciones:

- Discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
- Privación a los afectados de sus derechos y libertades o que se les pueda impedir ejercer el control sobre sus datos personales.
- Tratamiento no meramente incidental o accesorio de las categorías especiales de datos, de datos relacionados con infracciones o condenas penales o relacionados con la comisión de infracciones administrativas.
- Evaluación de aspectos personales de las personas afectadas con la finalidad de crear o utilizar sus perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

- Tratamiento de datos de grupos de afectados en una situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
- Tratamiento masivo que implique un gran número de afectados o comporte la recogida de una gran cantidad de datos personales.
- Tratamiento de datos personales que tengan que ser objeto de una transferencia, con carácter habitual, a terceros estados u organizaciones internacionales respecto de los cuales no se haya declarado un nivel adecuado de protección.
- Cualquier otra que, en opinión del responsable o del encargado, pueda tener relevancia y, en particular, las previstas en códigos de conducta y estándares definidos por esquemas de certificación.

El análisis de riesgos debe realizarse en todos los tratamientos, con independencia de que el tratamiento se tenga que someter o no a una evaluación de impacto sobre la protección de datos. Si se hace una evaluación de impacto sobre la protección de datos, el análisis de riesgos tiene que formar parte de él.

Con respecto a las medidas de seguridad que haya que adoptar para hacer frente a los riesgos que se identifiquen en el análisis, nos remitimos al apartado 7.7.5 de esta guía.

¿Qué metodología puede seguir un colegio profesional para evaluar los riesgos de un tratamiento?

De acuerdo con la disposición adicional primera de la LOPDGDD, el ENS determina las medidas de seguridad que hay que implantar para proteger los datos personales en las entidades del sector público. El ENS sólo exige el uso de una metodología de análisis de riesgos con reconocimiento internacional sin citar ninguna concreta.

La metodología Magerit es una de estas metodologías. El CCN-Cert (Centro Criptológico Nacional) ofrece varias herramientas que pueden ser útiles para la evaluación de riesgos.

¿Se pueden instalar programas informáticos que traten datos personales en dispositivos que son propiedad de los trabajadores del colegio, a fin de que puedan desarrollar las tareas que tienen encomendadas fuera de las instalaciones del colegio?

Dado que esta actuación puede entrañar riesgos tanto para la seguridad de los datos personales de los cuales es responsable el colegio, como para la privacidad de sus trabajadores, como paso previo a autorizar su uso (decisión que corresponde al colegio), es necesario hacer un análisis de riesgos e implementar las medidas técnicas y organizativas apropiadas para hacer frente a los riesgos detectados.
A efectos de garantizar la implementación de estas medidas, es recomendable recurrir a herramientas de gestión centralizada de dispositivos móviles (MDM). En el uso de estas herramientas hay que respetar la privacidad de los trabajadores.

Normativa aplicable: art. 32 RGPD; art. 28 LOPDGDD; ENS.

6.4 La evaluación de impacto y la consulta previa

Evaluación de impacto relativa a la protección de datos (EIPD)

Una evaluación de impacto en la protección de datos (EIPD) es un procedimiento que pretende identificar y controlar los riesgos para los derechos y las libertades de las personas, asociados a un tratamiento de datos.

El responsable tiene la obligación de hacer una evaluación del impacto en la protección de datos antes del tratamiento, cuando sea probable que por su naturaleza, alcance, contexto o fines suponga un alto riesgo para los derechos y libertades de las personas físicas, especialmente cuando se utilicen nuevas tecnologías. Por lo tanto, siempre hay que verificar este aspecto a la hora de determinar la necesidad de hacer o no una EIPD.

Entre otros supuestos, de acuerdo con el RGPD hay que hacer una evaluación de impacto en los siguientes:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento automatizado, como la elaboración de perfiles, sobre la base de la cual se toman decisiones que producen efectos jurídicos para las personas físicas o que las afectan significativamente de manera similar.
- Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales.
  A efectos de determinar si el tratamiento se hace a gran escala se pueden tener en cuenta los elementos siguientes:
  - El número de personas afectadas ya sea en términos absolutos o como proporción de una determinada población.
  - El volumen y la variedad de datos tratados.
  - La duración o permanencia de la actividad de tratamiento.
  - La extensión geográfica de la actividad de tratamiento.
- Observación sistemática a gran escala de una zona de acceso público.

Esta no es una lista cerrada.

Por otra parte, y de acuerdo con las previsiones del RGPD, la Autoridad Catalana de Protección de Datos ha elaborado y publicado en su página web una lista de tipos de tratamiento, no exhaustiva, para facilitar a los responsables de los tratamientos la identificación de los tratamientos que pueden requerir una evaluación de impacto. En la mayoría de los casos en los que el tratamiento cumpla con dos o más criterios de la lista, hay que realizar una EIPD. Cuantos más criterios reúna el tratamiento en cuestión, mayor es el riesgo que entraña el tratamiento y más certeza se tendrá de que hay que hacer una EIPD.

Actualmente se identifican los criterios siguientes:

- Tratamientos que implican perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (rendimiento en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.
- Tratamientos que implican la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de estas decisiones, incluyendo cualquier tipo de decisión que impida a una persona afectada ejercer un derecho o tener acceso a un bien o un servicio o formar parte de un contrato.
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control de la persona afectada de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permiten la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
- Tratamientos que implican el uso de categorías especiales de datos a que hace referencia el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permiten determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
- Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.
- Tratamientos que implican el uso de datos genéticos para cualquier fin.
- Tratamientos que implican el uso de datos a gran escala.
- Tratamientos que implican la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables diferentes.
- Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluidos datos de menores de 14 años, mayores de edad con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.
- Tratamientos que implican la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluida la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otros, de manera que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.
- Tratamientos de datos que impiden a las personas afectadas ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como tratamientos en que los datos han sido recopilados por un responsable diferente del que los tiene que tratar y en que es de aplicación alguna de las excepciones sobre la información que hay que proporcionar a las personas afectadas según el artículo 14.5 (b, c y d) del RGPD.

Como excepción, no hay que hacer una evaluación de impacto relativa a la protección de datos si el tratamiento está previsto en una disposición normativa y durante la tramitación del proyecto normativo ya se sometió a una EIPD.

La obligación de hacer la evaluación de impacto corresponde al responsable del tratamiento, con la colaboración del encargado del tratamiento y con el asesoramiento del delegado de protección de datos.

La evaluación tiene que incluir, como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de las finalidades del tratamiento, incluido, si procede, el interés legítimo perseguido.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento, en relación con su finalidad.
- Una evaluación de los riesgos para los derechos y las libertades de las personas afectadas.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garantizan la protección de datos personales y para demostrar la conformidad con la normativa de protección de datos, teniendo en cuenta los derechos y los intereses legítimos de las personas afectadas.

Sobre esta cuestión se recomienda consultar la Guía práctica sobre la evaluación de impacto relativa a la protección de datos y la Plantilla de evaluación de impacto relativa a la protección de datos, elaboradas por esta Autoridad.

Por otra parte, en la página web de la APDCAT también se puede descargar una aplicación para realizar la evaluación de impacto relativa a la protección de datos.

Consulta previa

Si de la evaluación de impacto en la protección de datos resulta que el tratamiento previsto puede infringir el RGPD o entrañaría un alto riesgo si no se toman medidas para mitigarlo, el responsable tiene que formular una consulta previa a la Autoridad Catalana de Protección de Datos, a través del trámite electrónico que figura en su sede electrónica.

La consulta debe ir acompañada, como mínimo, de la información siguiente:

- La evaluación de impacto realizada.
- Si procede, las responsabilidades respectivas del responsable, de los corresponsables y de los encargados implicados en el tratamiento, especialmente en caso de tratamiento dentro de un grupo empresarial.
- Las finalidades y los medios del tratamiento previsto.
- Las medidas y las garantías establecidas para proteger los derechos y las libertades de las personas afectadas.

- Los datos de contacto del delegado de protección de datos.
- Cualquier otra información que solicite la APDCAT.

La Autoridad tiene que asesorar por escrito al responsable en el plazo de ocho semanas desde la solicitud de consulta, prorrogable a seis semanas más indicando los motivos. La Autoridad puede hacer uso, si procede, de todos los poderes de investigación, correctivos, de autorización y consultivos que le confiere el RGPD, entre los cuales hay prohibir la operación de tratamiento.

¿Un colegio profesional tiene que hacer una evaluación de impacto si quiere utilizar datos biométricos para controlar la entrada a las instalaciones del colegio?

En caso de que la utilización de los datos biométricos se quiera iniciar o se haya iniciado con posterioridad al 25 de mayo de 2018, habría que hacer una evaluación de impacto relativa a la protección de datos de esta parte del tratamiento. Y si del resultado de la evaluación resulta una situación de alto riesgo, se tendría que plantear una consulta previa a la APDCAT, de acuerdo con el artículo 36 del RGPD. Si el tratamiento se ha iniciado antes de la fecha mencionada, a pesar de no ser obligatorio sería recomendable.

¿Los colegios profesionales tienen que publicar las EIPD que llevan a cabo?

El RGPD no establece la obligación de publicar las EIPD, aunque puede ser una buena práctica hacerlo, de manera completa o parcial, extrayendo las partes que puedan afectar a los derechos y libertades de las personas o a la seguridad del tratamiento. En cualquier caso, los responsables deben comunicarlo a la APDCAT si hacen una consulta previa, o si se lo solicita la Autoridad.

¿Hay que enviar a la Autoridad Catalana de Protección de Datos las evaluaciones de impacto relativas a la protección de datos?

No. Sólo tienen que comunicarse a la APDCAT en caso de que se realice una consulta previa, o si lo solicita la Autoridad.

Normativa aplicable: considerandos 84, 90 a 96; art. 35, 36 y 58 RGPD; art. 28 LOPDGDD.

6.5 El registro y el inventario de actividades del tratamiento

El registro de actividades del tratamiento es un instrumento documental que debe permitir tener una imagen actualizada de los tratamientos que lleva a cabo el colegio profesional. Es esencial para la gestión de riesgos, para el cumplimiento de los principios y las obligaciones, y para que la autoridad de control lo pueda supervisar.

El RGPD exceptúa de la obligación de llevar el registro de actividades del tratamiento a los responsables con menos de 250 empleados que sólo lleven a cabo tratamientos

ocasionales, que no impliquen el tratamiento de categorías especiales de datos o relativas a infracciones y condenas penales y que no puedan suponer un riesgo para los derechos y libertades de las personas afectadas. No obstante, los colegios profesionales siempre tendrán que llevar este registro, dada la amplitud de los tratamientos que deben realizar y su carácter no ocasional.

El registro de actividades de tratamiento, que tiene que constar en formato electrónico, debe incluir la información siguiente:

- Nombre y datos de contacto del responsable y, si procede, del corresponsable, así como del delegado de protección de datos.
- Finalidades del tratamiento.
- Descripción de las categorías de personas afectadas y las categorías de datos personales tratados.
- Categorías de destinatarios a los que se prevé comunicar los datos personales, incluidos los de terceros países u organizaciones internacionales, si procede.
- Si procede, transferencias internacionales de datos previstas, con identificación del tercer país u organización internacional de destino. Si se basa en garantías adecuadas, también hay que identificar la documentación donde constan.
- Plazos previstos para suprimir los datos, cuando sea posible.
- Descripción general de las medidas técnicas y organizativas de seguridad, cuando sea posible.

Los colegios profesionales tienen que hacer público en la sede electrónica o en la página web un inventario de sus actividades de tratamiento, accesible por medios electrónicos. En él debe constar la información del registro de actividades del tratamiento y su base legal, como mínimo para los tratamientos que se relacionen con el ejercicio de potestades de derecho público.

El registro y el inventario deben mantenerse actualizados, antes de iniciar el tratamiento y cada vez que se produzca un cambio significativo en el tratamiento. Hay que comunicar al delegado de protección de datos cualquier adición, modificación o exclusión en su contenido.

La APDCAT ha desarrollado y publicado en su web una aplicación para crear, mantener y gestionar el registro de las actividades de tratamiento, con la finalidad de ofrecer ayuda a los responsables del tratamiento. La aplicación permite dar de alta las diferentes actividades de tratamiento, así como modificarlas y darlas de baja cuando sea necesario. También permite generar un documento con las actividades de tratamiento que se han incluido en el registro, para poder publicarlo, si procede.

El registro tiene que estar a disposición de la Autoridad Catalana de Protección de Datos para el ejercicio de sus funciones como autoridad de control.

Cuando el colegio profesional actúe como encargado del tratamiento, también debe llevar un registro de actividades del tratamiento diferenciado, en el cual conste:

- El nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúa el encargado y, si procede, del representante del responsable o del encargado y del delegado de protección de datos.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- Las transferencias internacionales de datos personales previstas, incluida la identificación del tercer país u organización internacional de destino. Si se basa en garantías adecuadas, también hay que identificar la documentación donde constan.
- La descripción general de las medidas técnicas y organizativas de seguridad (cuándo sea posible).

¿Cómo puede el colegio organizar el registro de actividades del tratamiento?

Una posibilidad para organizar este registro es partir de los ficheros que el colegio había notificado al Registro de Protección de Datos de Cataluña, y detallar todas las operaciones que se efectúan sobre cada conjunto estructurado de datos.

También se puede organizar entorno a operaciones de tratamiento concretas, vinculadas a una finalidad básica común de todas ellas (por ejemplo “registro de colegiados”, “gestión contable” o “gestión de recursos humanos y nóminas”), o bien de acuerdo con otros criterios diferentes.

Un colegio profesional se plantea comunicar a una asociación mundial de profesionales datos de representantes de asociaciones culturales del municipio, con su consentimiento. ¿Eso podría afectar a la información del registro de actividades de tratamiento?

Sí. El registro de actividades de tratamiento tiene que incluir cuáles son los destinatarios de los datos, incluidos los de terceros países, así como las transferencias internacionales de datos que se puedan producir. Si el registro no lo preveía se tendría que incorporar, ya que supone un cambio significativo del tratamiento inicial.

¿Los tratamientos que lleva a cabo la comisión de cultura del colegio profesional y de la cual es responsable la comisión de cultura, deben incluirse en el registro de actividades del tratamiento del colegio?

Los tratamientos que lleva a cabo tienen que incluirse en el registro de actividades de tratamiento del responsable del tratamiento. No obstante, nada impide que dentro de una misma organización todos los tratamientos puedan formar parte de un mismo registro, siempre que quede claro quién es el responsable de cada uno.

¿Cómo se tiene que publicar el inventario de actividades de tratamiento por medios electrónicos?

Los colegios profesionales tienen que hacer público el inventario en su sede electrónica o en su página web y hacer constar la información del registro de actividades del tratamiento y su base legal. Eso, como mínimo para los tratamientos relacionados con el ejercicio de potestades de derecho público, tanto si actúa como responsable, como si lo hace como encargado del tratamiento.

¿Hay que notificar a la Autoridad Catalana de Protección de Datos los tratamientos inscritos en el registro de actividades de tratamiento?

No. El registro tiene que estar a disposición de la Autoridad Catalana de Protección de Datos para el ejercicio de sus funciones como autoridad de control, pero no hay que notificar los tratamientos que se inscriben.

Normativa aplicable: considerando 82, art. 30 RGPD; 31, 77.1.g) y DF 11ª LOPDGDD; 6.bis LT.

7. Obligaciones del responsable del tratamiento y del encargado durante el tratamiento

Las personas afectadas disponen de una serie de derechos durante el tratamiento de los datos:

- Derecho a ser informadas sobre el tratamiento y sus principales elementos
- Derecho de acceso
- Derecho de rectificación
- Derecho de supresión
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad
- Derecho de oposición
- Derecho a no ser objeto de decisiones automatizadas

Además, el responsable del tratamiento tiene que cumplir una serie de obligaciones y garantías, orientadas a asegurar la adecuación del tratamiento a la normativa vigente. Estas obligaciones son de aplicación durante la recogida, el almacenaje, la utilización o la comunicación de los datos personales y, en algún caso (deber de confidencialidad), incluso después de que finalice la relación jurídica. Dichas obligaciones son:

- Formalizar el encargo del tratamiento.
- Nombrar al delegado de protección de datos.
- Cumplir el régimen de transferencias internacionales de datos.
- Garantizar la seguridad de los datos: integridad y confidencialidad.
- Aprobar una política de protección de datos.

Además, en virtud del principio de responsabilidad proactiva, el responsable del tratamiento tiene que adoptar cualquier otra medida para garantizar el cumplimiento de los principios de la normativa de protección de datos y hacer frente a los riesgos que se puedan generar para los derechos y libertades de las personas físicas. En especial, destacan la promoción y/o adhesión a los códigos de conducta y la obtención de certificados, sellos o marcas en materia de protección de datos.

7.1 La información a las personas afectadas

Las personas afectadas tienen derecho a ser informadas sobre las condiciones en que el responsable llevará a cabo el tratamiento de sus datos, sin necesidad de solicitarlo.

Corresponde al responsable del tratamiento cumplir esta obligación y estar en condiciones de demostrar que lo ha cumplido.

La información debe ser:

- Concisa, transparente, inteligible y de fácil acceso.
- En un lenguaje claro y sencillo, especialmente cuando la información se dirige a un menor. Hay que evitar las fórmulas enrevesadas y que incorporen remisiones a textos legales o que no se distingan de la información sobre otras cuestiones.
- Por escrito o por otros medios, incluidos los electrónicos.
- Facilitada de modo que el responsable pueda acreditar que lo ha facilitado.

Con respecto al contenido de la información, hay que diferenciar si los datos se obtienen de la persona afectada o no.

Si los datos se obtienen de la persona afectada, en el momento de su obtención hay que informarla sobre:

- La identidad y datos de contacto del responsable y, si procede, de su representante.
- Los datos de contacto del delegado de protección de datos.
- Las finalidades y la base jurídica del tratamiento.
- Los intereses legítimos perseguidos en que se fundamenta el tratamiento, si procede.
- Los destinatarios o categorías de destinatarios de los datos, si procede.
- La intención de transferir los datos a un tercer país o a una organización internacional y el instrumento para hacerlo, así como el lugar donde se puede obtener una copia de las garantías adecuadas, si procede.
- El plazo durante el cual se conservarán los datos, o los criterios para determinarlo.
- El derecho a solicitar el acceso a los datos, la rectificación o la supresión de los datos, la limitación del tratamiento, la oposición al tratamiento y la portabilidad de los datos.

- El derecho a retirar en cualquier momento el consentimiento que se ha prestado, si el tratamiento se fundamenta en esta base jurídica.
- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato, y si la persona afectada está obligada a facilitar los datos y las consecuencias de no facilitarlos.
  Asimismo, cuando se recogen datos relativos a la ideología, la religión o las creencias, hay que advertir expresamente a la persona afectada de su derecho a no facilitar estos tipos de datos.
- El derecho a presentar una reclamación ante una autoridad de control.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y la información sobre la lógica aplicada y sus consecuencias.

Si los datos no se obtienen de la persona afectada, además de los aspectos que se acaban de relacionar también hay que informarla de:

- Las categorías de datos personales que se tratan.
- La fuente de donde proceden los datos personales.

En ambos casos, la LOPDGDD ha previsto la posibilidad de utilizar un mecanismo de doble capa para informar a las personas afectadas. En la primera capa, que se puede incluir por ejemplo en los formularios de recogida de datos, tiene que constar la información básica junto con una remisión a una dirección electrónica u otro medio que permita a la persona afectada acceder de manera sencilla a la segunda capa, con el resto de información prevista en el RGPD.

Cuando los datos se obtienen directamente de la persona afectada, la primera capa tiene que incluir:

- La identidad del responsable del tratamiento y de su representante, si procede.
- La finalidad del tratamiento.
- La posibilidad de ejercer los derechos.

Cuando los datos no se obtienen directamente de la persona afectada, la primera capa también debe incluir:

- Las categorías de datos objeto de tratamiento.
- Las fuentes de las cuales proceden los datos.

La información debe ponerse a disposición de las personas afectadas en el **plazo siguiente**:

- Si los datos se obtienen de la persona afectada, en el momento en que se solicitan los datos.

- Si los datos no se obtienen de la persona afectada, en un plazo razonable, no superior a un mes, a no ser que haya que hacerlo con anterioridad porque concurre alguna de las causas siguientes:
  - Si los datos se tienen que utilizar para comunicarse con la persona afectada, hay que informar antes o en la primera comunicación con ella.
  - Si está previsto comunicarlas a otro destinatario, hay que informar antes o en el momento de esta comunicación.

Excepciones al deber de informar:

a) Cuando los datos se obtienen de la persona afectada, no hay que informar si:

   - La persona afectada ya dispone de la información.
   - Puede afectar a la defensa nacional, la seguridad pública o la persecución de infracciones penales.

b) Cuando los datos no se obtienen de la persona afectada, no hay que informar si:

   - Es imposible o supone un esfuerzo desproporcionado (en particular, en caso de tratamientos con finalidades de archivo o estadísticos o de investigación científica o histórica), o imposibilita u obstaculiza gravemente los objetivos del tratamiento.
   - Hay una previsión legal expresa del tratamiento (obtención o comunicación que ha comportado la recogida de los datos).
   - Hay una obligación de secreto legal.
   - Puede afectar a la defensa nacional, la seguridad pública o la persecución de infracciones penales.

También hay que tener en cuenta que la Ley Orgánica 7/2021 establece que no se debe informar de las comunicaciones de datos que se realicen para atender los requerimientos de información de los órganos judiciales, el ministerio fiscal y la policía judicial, para la investigación o el enjuiciamiento de infracciones penales o la ejecución de las penas, o con finalidades de prevención y protección ante un peligro real y grave para la seguridad pública.

En los anexos de esta guía se ofrecen modelos de cláusulas informativas que, en cualquier caso, hay que adaptar a las circunstancias del tratamiento concreto que se pretende llevar a cabo:

- Anexo 1: Modelo de cláusula informativa para documentos de recogida de datos por el colegio profesional
- Anexo 2: Modelo de cláusula informativa para actualizar los datos que aparecen en la lista o guía de personas colegiadas

Sobre esta cuestión, se recomienda consultar la Guía para el cumplimiento del deber de informar en el RGPD publicada por esta Autoridad.

¿Qué información deben dar los colegios profesionales a los colegiados, sobre los datos recogidos para elaborar la guía o la lista profesional y su publicación posterior?

El colegio tiene que informar de los aspectos previstos en los artículos 13 y 14 del RGPD y en el artículo 11 de la LOPDGDD. En especial, conviene informar sobre los datos que se difundirán en cumplimiento de la obligación de poner a disposición de las personas usuarias y consumidoras destinatarias de los servicios profesionales determinada información a través de la ventanilla única.

¿Qué medio puede utilizar el colegio profesional para cumplir con el deber de información previamente a la recogida de datos?

El deber de información se puede cumplir de varias formas, como incluir la cláusula informativa en los formularios, impresos o cuestionarios utilizados en la recogida de datos. Si no se pueden utilizar formularios, y las circunstancias lo justifican, se pueden colocar carteles informativos en los puntos de recogida de los datos, que sean claramente visibles y accesibles para los colegiados. La información incluida en los carteles tiene que ser completa y detallada. En todo caso, hay que cumplir con lo que disponen los artículos 13 a 14 del RGPD y, si procede, el artículo 11 de la LOPDGDD.

¿Si, en el marco de un procedimiento en ejercicio de sus funciones públicas, un colegio profesional tiene que consultar datos que ya estaban en poder de una administración pública, debe informar a las personas afectadas?

Sí. Si al amparo del artículo 28.2 de la LPAC un colegio profesional consulta datos que estén en poder de otra administración, tiene que informar a las personas afectadas sobre esta consulta y de la posibilidad de oponerse.

¿Cuándo no hay que pedir el consentimiento, hay que informar igualmente a las personas afectadas?

Sí. El deber de información debe cumplirse en todos los casos, a menos que concurra alguna de las excepciones que prevé el RGPD.

¿Hay que incluir la cláusula informativa en todos los correos electrónicos que envía el colegio profesional a los colegiados?

No. No es obligatorio, si ya se informó en el momento de la recogida de los datos. Pero puede ser recomendable incluirla, así como tenerla a disposición de las personas afectadas a través de la página web, a fin de que las personas que se relacionan con el colegio conozcan dónde están sus datos, el tratamiento que se hace, quién es el responsable y cómo pueden ejercer sus derechos.

Normativa aplicable: considerandos 58, 60 a 62 y art.12, 13 y 14 RGPD; art. 11 y DA 14ª LOPDGDD; art. 24 LOPD; art. 7 de la Ley Orgánica 7/2021.

7.2 La atención de los derechos de las personas afectadas

7.2.1 Aspectos comunes

El RGPD reconoce a la persona afectada el poder de control sobre sus datos personales y le otorga la posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individuales automatizadas.

También establece el derecho a ser informado sobre el tratamiento. No obstante, dado que no requiere una solicitud de las personas afectadas, sino que el responsable está obligado a cumplirlo directamente sin que haya que solicitarlo, este derecho se analiza de manera específica en el apartado 7.1 de esta guía.

El responsable del tratamiento tiene que facilitar el ejercicio de estos derechos y debe adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos personales, y las que atienden al público, puedan informar del procedimiento que deben seguir las personas afectadas para ejercer sus derechos.

Se trata de derechos personalísimos. Por lo tanto, tiene que ejercerlos la misma persona afectada o un tercero por representación, ante el responsable del tratamiento.

Solicitud

- La solicitud se puede presentar por cualquier medio que permita dejar constancia de la identidad de la persona que la formula y de su presentación.

  Hay que posibilitar la presentación de solicitudes por medios electrónicos, especialmente cuando los datos se tratan por estos medios. En este caso, si es posible, la información debe facilitarse en este formato, a menos que la persona afectada solicite que se le entregue de otra manera.

- El responsable tiene que tomar las medidas razonables para verificar la identidad de la persona afectada que ejerce un derecho. Si tiene dudas razonables en cuanto a la identidad de quien presenta la solicitud, puede pedir información adicional para confirmarla.
- El responsable no está obligado a mantener, obtener o tratar información adicional con el fin de identificar a la persona afectada con la única finalidad de poder atender las solicitudes de ejercicio de derechos. Si los datos personales que trata no le permiten relacionar la información con la persona afectada que ejerce el derecho, debe informarla sobre esta circunstancia. En este caso, los derechos reconocidos

por el RGPD no son de aplicación, a no ser que la persona afectada facilite información adicional que permita la identificación.

- En caso de que el responsable no curse la solicitud de la persona afectada en el plazo de un mes desde su recepción, debe informarla de las razones por las cuales no ha actuado, así como de la posibilidad de presentar una reclamación ante la autoridad de control y de ejercer acciones judiciales.
- El ejercicio de cualquiera de estos derechos tiene carácter gratuito. No obstante, si las solicitudes son infundadas o excesivas, especialmente porque son repetitivas, el responsable puede cobrar un canon razonable según los costes administrativos que se deriven de facilitar la información, la comunicación o la actuación solicitada, o se puede negar a actuar ante la solicitud. Corresponde al responsable demostrar el carácter infundado o excesivo de la solicitud. A estos efectos, se puede considerar repetitivo el ejercicio del derecho de acceso más de una vez en el plazo de seis meses, a no ser que exista una causa legítima para hacerlo.
- El responsable puede contar con la colaboración de los encargados para atender las solicitudes de ejercicio de los derechos. Esta colaboración debe estar establecida en el contrato de encargo de tratamiento.
- Hay que atender la solicitud de ejercicio del derecho sin dilación indebida y en cualquier caso en el plazo máximo de un mes desde que se recibió, prorrogable dos meses más si es necesario, según la complejidad y el número de solicitudes. En caso de prórroga, hay que informar a la persona afectada dentro del plazo del primer mes, e indicar los motivos de la dilación.

En los anexos 3, 4, 5, 6 y 7 de esta guía pueden encontrarse modelos para ejercer los derechos de acceso, rectificación, supresión, oposición y limitación.

Limitación de los derechos

Estos derechos sólo pueden limitarse mediante una norma con rango de ley o el derecho de la Unión, que respete los derechos y las libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

- La seguridad del Estado.
- La defensa.
- La seguridad pública.
- La prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales.
- Otros objetivos importantes de interés público general de la Unión Europea o de un estado miembro (económico, financiero, fiscal, presupuestario y monetario, sanidad pública, seguridad social).
- La protección de la independencia judicial y de los procedimientos judiciales.
- La prevención, investigación, detección y enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas.

- La supervisión, inspección o reglamentación vinculada con el ejercicio de la autoridad pública en cualquiera de los supuestos mencionados en los apartados anteriores.
- La protección de la persona afectada o de los derechos y las libertades de otros.
- La ejecución de demandas civiles.

Así, por ejemplo, el artículo 23 de la LOPD, que la LOPDGDD mantiene vigente, establece que se puede denegar el ejercicio de los derechos de acceso, rectificación o cancelación (supresión):

- En función de los peligros que se puedan derivar para la defensa del Estado o la seguridad pública, la protección de los derechos y las libertades de terceros o las necesidades de las investigaciones que se estén llevando a cabo.
- Cuando los responsables de los ficheros de la hacienda pública consideren que eso puede obstaculizar las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando la persona afectada esté siendo objeto de actuaciones inspectoras.

Reclamación de tutela de derechos

Para ejercer sus derechos, el ciudadano debe dirigirse al responsable del tratamiento. Si no se da respuesta a la solicitud en el plazo de un mes (a menos que haya sido ampliado), o se deniega el ejercicio de uno de estos derechos, puede dirigirse a la Autoridad Catalana de Protección de Datos mediante una reclamación de tutela de derechos.

La tutela de los derechos reconocidos por el RGPD se ejerce mediante un procedimiento que se tramita ante la Autoridad Catalana de Protección de Datos y que se inicia a instancia de la persona afectada.

La Autoridad traslada la reclamación al responsable del tratamiento y, una vez recibidas las alegaciones dentro del plazo legalmente establecido y practicadas todas las pruebas, tiene que dictar resolución y notificarla, en el plazo de 6 meses desde la fecha de entrada de la reclamación. Si no se resuelve dentro de este plazo, la reclamación de tutela se considera desestimada.

Cuando la resolución de la reclamación es estimatoria, la Autoridad Catalana de Protección de Datos requiere al responsable del tratamiento para que, en el plazo de los 10 días siguientes a la notificación, haga efectivo el ejercicio del derecho reclamado.

¿Hay que atender la solicitud de las personas afectadas que no hayan utilizado el medio establecido por el responsable?

Sí, el ejercicio del derecho no se puede denegar por el solo motivo de que la persona afectada opte por otro medio.

¿El responsable del tratamiento puede excluir la posibilidad de ejercer los derechos a través del correo electrónico?

No, la persona interesada puede solicitar que el derecho de acceso se haga efectivo a través del correo electrónico y tiene derecho a recibir la información en este mismo formato. Ahora bien, hay que tener en cuenta que si el colegio ofrece un determinado sistema para hacer efectivo el derecho de acceso y la persona afectada lo rechaza, el colegio no tiene que responder de los riesgos para la seguridad de la información que pueden derivar de la elección.

¿Hay que responder la solicitud cuando no se dispone de datos o ya se han destruido?

Sí, siempre hay que dar respuesta a las solicitudes de ejercicio de los derechos, sin dilación indebida y dentro del plazo máximo de un mes, a menos que se haya acordado la prórroga.

Normativa aplicable: art. 11, 12, 23 y 77 RGPD; art. 12 a 18 y DA 14ª LOPDGDD; art. 23 LOPD; art. 5.b) y 16 LACPD; art. 117 y s. RLOPD.

7.2.2 Derecho de acceso

La persona afectada tiene derecho a saber si el responsable del tratamiento trata sus datos personales y, en ese caso, tiene derecho a acceder a estos datos y a obtener la información siguiente:

- Las finalidades del tratamiento.
- Las categorías de datos personales que se tratan.
- Los destinatarios o las categorías de destinatarios a las que se han comunicado o se comunicarán los datos.
- El plazo previsto de conservación de los datos personales o los criterios utilizados para determinarlo.
- El derecho a solicitar al responsable del tratamiento la rectificación o la supresión de los datos, la limitación del tratamiento o el derecho a oponerse.
- El derecho a presentar una reclamación ante la autoridad de control competente.
- El origen de los datos, cuando no se han obtenido de la persona afectada.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias de este tratamiento.

- En caso de transferencias internacionales de datos, las garantías adecuadas que se ofrecen.

Además, tiene derecho a obtener una copia gratuita de los datos objeto del tratamiento, siempre que no afecte negativamente a los derechos y las libertades de otros. Para copias posteriores, se puede establecer un canon según los costes administrativos.

El derecho de acceso se puede ejercer en relación con datos concretos o con la totalidad de los datos sometidos a tratamiento.

En casos de especial complejidad, el responsable del tratamiento puede facilitar a la persona afectada una lista de sus tratamientos y pedirle que especifique respecto de cuáles ejerce su derecho.

La persona afectada puede solicitar que el derecho de acceso se haga efectivo a través de los sistemas de consulta siguientes:

- Visualización en pantalla.
- Escrito, copia o fotocopia, por correo certificado u ordinario.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema que sea adecuado a las características del tratamiento.

Si se solicita por medios electrónicos, la persona afectada tiene derecho a recibir la información en este mismo formato.

Si el colegio ofrece un determinado sistema para hacer efectivo el derecho de acceso y la persona afectada lo rechaza, el colegio no tiene que responder de los riesgos para la seguridad de la información que se pueden derivar de la elección.

¿Cómo puede un colegiado conocer la información que tiene un colegio profesional sobre su persona?

El colegiado puede conocer esta información ejerciendo el derecho de acceso, mediante una solicitud dirigida al colegio correspondiente.

¿Es posible denegar el ejercicio del derecho de acceso por la dificultad o el elevado coste que puede suponer al colegio profesional?

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente por su carácter repetitivo, el responsable puede cobrar un canon o inadmitir la solicitud. A estos efectos, se puede considerar repetitivo ejercer el derecho de acceso más de una vez en el plazo de seis meses, a no ser que haya una causa legítima para hacerlo.

Si la persona afectada escoge un medio diferente al que se le ofrece, que supone un coste desproporcionado, la solicitud debe considerarse excesiva, por lo cual la persona afectada tiene que asumir el exceso de costes que conlleva su elección.

¿Los herederos de una persona colegiada difunta pueden ejercer, en su nombre, el derecho de acceso a sus datos en poder del colegio?

La normativa de protección de datos no es aplicable al tratamiento de datos de personas difuntas. Ahora bien, la LOPDGDD prevé expresamente que determinadas personas que están vinculadas a ellas "por razones familiares o de hecho", pueden acceder a la información relativa a la persona difunta y, si procede, pedir la rectificación o la supresión.

Eso, a menos que conste la prohibición expresa del titular de la información o que determinadas previsiones legales puedan limitar el ejercicio de esta facultad.

Eso puede incluir también el acceso de los herederos a una cuenta de correo facilitada por el colegio.

¿En el caso de un profesional difunto, el despacho profesional al cual pertenecía puede acceder a la información de la cuenta de correo facilitada por el colegio profesional?

El despacho profesional de la persona difunta únicamente puede acceder a los datos de esta persona si ha estado expresamente habilitado a este efecto, en un documento de voluntades digitales u otra autorización.

Hay que recordar la conveniencia de aprobar normas de utilización del sistema de correo electrónico de los colegios profesionales, que hayan sido aprobadas y aceptadas por sus usuarios y que prevean, además de los sistemas de acceso al correo, las condiciones de uso y de conservación y otras eventualidades, como el destino de la información en caso de defunción, que sean aplicables en ausencia de manifestación expresa de la persona interesada.

Normativa aplicable: art. 15 RGPD; art. 3, 12 y 13 LOPDGDD; art. 28 RLOPD.

7.2.3 Derecho de rectificación

La persona afectada tiene derecho a obtener la rectificación de sus datos personales que sean inexactos y a que se completen sus datos incompletos.

El responsable debe:

- Comunicar la rectificación efectuada a cada uno de los destinatarios a quienes se hayan comunicado los datos, a no ser que sea imposible o exija un esfuerzo desproporcionado.
- Informar a la persona afectada sobre los destinatarios, si lo solicita.

La rectificación de los datos da lugar al bloqueo de los datos rectificados. Al respecto nos remitimos al apartado 8.2 de esta guía.

¿Un colegiado puede solicitar la rectificación de los datos que aparecen en la guía o lista de profesionales?

Sí, indicando los datos erróneos que hay que corregir y aportando la documentación que lo acredita.

¿Cuál es el plazo para resolver y notificar una solicitud de rectificación?

La solicitud de rectificación tiene que resolverse y notificarse en el plazo máximo de un mes a contar a partir de la fecha de recepción de la solicitud. Este plazo se puede prorrogar dos meses más (tres, en total), teniendo en cuenta la complejidad o el número de solicitudes.

Normativa aplicable: art. 16 y 19 RGPD; 14 y 32 LOPDGDD.

7.2.4 Derecho de supresión

La persona afectada tiene derecho a obtener la supresión de sus datos personales ("derecho al olvido"), cuando:

- Los datos ya no son necesarios para la finalidad para la que se recogieron.
- Se retira el consentimiento en el cual se basaba el tratamiento.
- La persona afectada se opone al tratamiento.
- Los datos se tratan ilícitamente.
- Los datos tienen que suprimirse para cumplir una obligación legal.
- Los datos se han obtenido en relación con la oferta de servicios de la sociedad de la información dirigida a menores.

Si el responsable ha comunicado los datos, es necesario que:

- Adopte medidas razonables, a no ser que sea imposible o exija esfuerzos desproporcionados, por informar de la supresión a los destinatarios que están tratando estos datos, a fin de que, si procede, los supriman. Cuando se hayan hecho públicos, tiene que adoptar las medidas razonables, incluidas medidas técnicas, para informar a los responsables que los están tratando de la solicitud del afectado de suprimir cualquier enlace o copia de los datos.
- Informe a la persona afectada sobre los destinatarios, si lo solicita.

Cuando la supresión derive del ejercicio del derecho de oposición al tratamiento para finalidades de marketing directo, el responsable puede conservar los datos identificativos de la persona afectada necesarios con la finalidad de impedir tratamientos futuros para esta finalidad.

El derecho de supresión no se aplica cuando el tratamiento es necesario para:

- El ejercicio del derecho a la libertad de expresión e información.
- El cumplimiento de una obligación legal, o para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
- Razones de interés público en el ámbito de la salud.
- La existencia de finalidades de archivo en interés público, de investigación científica o histórica o finalidades estadísticas.
- La formulación, el ejercicio o la defensa de reclamaciones.

La supresión de los datos da lugar al bloqueo de los datos suprimidos. Al respecto, nos remitimos al apartado 8.2 de esta guía.

¿Un colegio profesional está obligado a suprimir los datos bancarios que había facilitado un colegiado para pagar las cuotas, si el colegiado lo solicita?

Sí, si ya no son necesarios. No se pueden suprimir si es imprescindible mantenerlos para cobrar las cuotas derivadas de la relación jurídica establecida entre el colegiado y el colegio profesional –por ejemplo, porque la normativa colegial establece únicamente este sistema de pago.

¿Los herederos pueden ejercer el derecho de supresión de datos de la persona difunta?

La LOPDGDD prevé expresamente que determinadas personas vinculadas con la persona difunta "por razones familiares o de hecho" puedan solicitar la rectificación o la supresión de los datos de la persona difunta. Eso, a menos que conste la prohibición expresa del titular de la información o que determinadas previsiones legales puedan limitar el ejercicio de esta facultad.

Normativa aplicable: art. 17 y 19 RGPD; 3, 15 y 32 LOPDGDD.

7.2.5 Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento consiste en marcar los datos personales, con la finalidad de limitar el tratamiento en el futuro sólo para determinadas finalidades. No se tiene que confundir con el bloqueo de datos.

Se puede solicitar la limitación:

- Cuando la persona afectada ha ejercido los derechos de rectificación u oposición y mientras el responsable determina si procede atender la solicitud.
- Cuando el tratamiento es ilícito, pero la persona afectada se opone a la supresión y solicita la limitación.

- Cuando los datos son innecesarios para el tratamiento, pero la persona afectada se opone a la supresión porque los necesita para formular, ejercer o defender reclamaciones.

Mientras dura la limitación, el responsable sólo puede tratar los datos, más allá de conservarlos, en los casos siguientes:

- Con el consentimiento de la persona afectada.
- Para formular, ejercer o defender reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.
- Por razones de interés público importantes de la Unión o del estado miembro.

Cuando una persona afectada ha obtenido la limitación del tratamiento, hay que informarla antes de que se levante la medida.

Cuando se ha limitado el tratamiento, el responsable debe:

- Hacer constar la limitación de forma clara en sus sistemas de información.
- Comunicar la limitación efectuada a cada uno de los destinatarios a quienes se hayan comunicado los datos, a no ser que resulte imposible o exija un esfuerzo desproporcionado.
- Informar a la persona afectada sobre los destinatarios, si lo solicita.

Normativa aplicable: art. 18 RGPD; 16 LOPDGDD.

7.2.6 Derecho a la portabilidad

En virtud del derecho a la portabilidad, la persona afectada tiene derecho a recibir, en un formato estructurado, de uso común y de lectura mecánica, sus datos personales que ha facilitado a un responsable del tratamiento.

Este derecho también incluye la posibilidad de que se transmitan directamente del responsable a otro responsable, si es técnicamente posible.

Para que el derecho de portabilidad sea aplicable, es necesario que se cumplan las condiciones siguientes:

- La recogida de los datos se basó en el consentimiento o en un contrato.
- El tratamiento se realiza con medios automatizados.

Limitaciones:

- No se puede ejercer este derecho cuando el tratamiento se fundamenta en el cumplimiento de una misión de interés público o es inherente al ejercicio de poderes

públicos. Por lo tanto, no es aplicable cuando el colegio profesional actúa en ejercicio de sus funciones públicas.

- No puede afectar negativamente a los derechos y libertades de otras personas.

¿Se puede ejercer el derecho de portabilidad en el ámbito de los colegios profesionales?

Sólo se puede ejercer cuando el tratamiento se basa en el consentimiento de la persona afectada o cuando el tratamiento sea necesario para ejecutar un contrato en el cual la persona afectada es parte o bien para aplicar medidas precontractuales a petición suya. No se puede ejercer cuando el tratamiento es necesario para ejercer una misión en interés público o para ejercer potestades públicas.

¿Cuándo se solicita la portabilidad a un colegio profesional en relación con un tratamiento de datos derivado de las funciones públicas del colegio, hay que responder a la persona afectada, teniendo en cuenta que el derecho de portabilidad no se aplica en este caso?

Sí. Aunque el derecho a la portabilidad en principio no tiene que prosperar, en relación con los tratamientos que llevan a cabo los colegios profesionales para ejercer sus funciones públicas, siempre hay que atender cualquier solicitud y dar respuesta dentro del plazo pevisto.

¿Es necesario que en las cláusulas informativas de protección de datos que el colegio dirige a las personas afectadas se indique la posibilidad de ejercer el derecho de portabilidad?

El colegio debe informar sobre la posibilidad de ejercer el derecho a la portabilidad cuando la base jurídica del tratamiento sea el consentimiento o la ejecución de un contrato. Cuando la base jurídica del tratamiento sea otra, como el cumplimiento de una obligación legal, el ejercicio de una potestad pública o el cumplimiento de una misión en interés público, la información sobre la posibilidad de ejercer este derecho no debe incluirse, ya que no es posible ejercerlo.

Normativa aplicable: art. 20 RGPD; 17 LOPDGDD.

7.2.7 Derecho de oposición

La persona afectada tiene derecho a oponerse, en cualquier momento, al tratamiento de sus datos personales en los supuestos siguientes:

- Cuando el tratamiento se basa en una **misión realizada en interés público** o en **el ejercicio de poderes públicos conferidos al responsable**, o en el **interés legítimo** perseguido por el responsable del tratamiento o por un tercero. En este caso, la oposición se tiene que fundamentar en motivos relacionados con su situación personal. El responsable del tratamiento debe dejar de tratarlos, a no ser que acredite motivos legítimos imperiosos que prevalezcan sobre los intereses, los

derechos y las libertades de la persona afectada, o para formular, ejercer o defenderse de reclamaciones.
- Cuando el tratamiento tiene por objeto el **marketing directo**, incluida la elaboración de perfiles relacionados con el marketing.
- Cuando el tratamiento tiene **fines estadísticos** o de **investigación científica o histórica** y se invoca un motivo relacionado con su situación personal, a menos que sea necesario para el cumplimiento de una misión en interés público.

En el ámbito de los servicios de la sociedad de la información, las personas afectadas tienen que poder ejercer este derecho por medios automatizados.

¿Un colegiado puede oponerse a la publicación de sus datos personales en la guía o lista de profesionales, sin causa justificada?

El colegiado puede oponerse a este tratamiento, si alega motivos relativos a su situación personal, como por ejemplo razones de seguridad, sufrir algún tipo de amenaza, etc. En este caso, una vez realizada la ponderación con los intereses que justifican la publicación, el colegio debe excluirlo del listado profesional, a menos que haya motivos legítimos imperiosos que justifiquen que se mantengan publicados.

Con respecto a la posibilidad de pedir que se excluyan sus datos del listado de profesionales del colegio de la utilización para finalidades de publicidad o prospección comercial, en este caso no hay que alegar ninguna situación personal, sino que es suficiente solicitarlo.

Normativa aplicable: art. 21 RGPD.

7.2.8 Derecho a no ser objeto de decisiones automatizadas

La persona afectada tiene derecho a no ser objeto de una decisión basada sólo en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ella o que le afecte negativamente.

Sólo se pueden adoptar estas decisiones en los supuestos siguientes:

a) Si es necesario **para formalizar o ejecutar un contrato** entre la persona afectada y un responsable de tratamiento.
b) Si está autorizado por una **norma con rango de ley** o por el derecho de la Unión que establezca garantías adecuadas para los derechos y libertades de las personas afectadas.
c) Si se basa en el **consentimiento** explícito de la persona afectada.

Garantías exigibles:

- En los tres casos, hay que establecer medidas adecuadas para salvaguardar los derechos, las libertades y los intereses legítimos de la persona afectada.
- En los casos de las letras *a)* y *c)*, la persona afectada tiene derecho a:
  - Obtener intervención humana por parte del responsable.
  - Expresar su punto de vista.
  - Impugnar la decisión.

- Las decisiones no se pueden basar en categorías especiales de datos, a menos que:

  - Se disponga del consentimiento de la persona afectada.
  - Haya que tratarlos por razones de interés público esencial establecido por una ley o el derecho de la Unión.

Normativa aplicable: art. 22 RGPD.

7.3 La exactitud y la actualización de los datos

Los datos tienen que ser exactos y, si es necesario, deben actualizarse. El responsable tiene que adoptar de oficio todas las medidas razonables para que los datos personales inexactos se supriman o se rectifiquen, sin dilación. También los puede tener que rectificar, cuando proceda, como consecuencia de que las personas afectadas hayan ejercido el derecho de rectificación.

Eso hace necesario que, para mantener la información actualizada, el colegio profesional tenga que disponer de unos mecanismos individualizados de actualización a instancia de las personas interesadas, así como procedimientos masivos periódicos de actualización y, si procede, de supresión de los datos.

La inexactitud de los datos no es imputable al responsable del tratamiento si los ha obtenido:

- Directamente de la persona afectada.
- De un mediador o responsable, si las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecen la posibilidad de que un intermediario o mediador recoja en nombre propio los datos de las personas afectadas, para transmitirlos al responsable. El mediador o intermediario asume las responsabilidades que se puedan derivar si los datos que comunica al responsable no se corresponden con los que ha facilitado la persona afectada.
- De otro responsable, en virtud del derecho a la portabilidad ejercido por la persona afectada.
- De un registro público.

Los datos rectificados están sometidos al deber de bloqueo. Al respecto, nos remitimos al apartado 8.2 de esta guía.

Actualización de las listas de profesionales

Tanto la normativa de protección de datos como la normativa sectorial obligan a los colegios profesionales, como responsables del tratamiento, a verificar periódicamente que los datos publicados se adecuan a la realidad de los colegiados. Hay que hacerlo a través de un procedimiento que permita comprobar si los datos son correctos, y modificar la guía en caso de baja o defunción de algún colegiado. Esta revisión periódica es independiente de la obligación de atender las solicitudes de rectificación o supresión de las personas afectadas.

- **Verificación de la actualización de datos de la lista de profesionales colegiados:** se recomienda que antes de publicar una nueva edición de la lista o guía profesional, el colegio informe a los colegiados de los datos que contendrá la guía o listado y les ofrezca la posibilidad de solicitar la rectificación de los datos incorrectos y de oponerse a que alguno o todos sus datos aparezcan en la lista.

Los colegiados también tienen derecho a solicitar que se excluya el uso de sus datos personales para finalidades de publicidad o prospección comercial. Por lo tanto, el colegio también tiene que informar de esta posibilidad, en el momento de realizar la comunicación para actualizar los datos.

En el anexo 2 de esta guía se puede encontrar un modelo de la cláusula informativa para actualizar los datos que aparecen en la lista o guía de personas colegiadas.

- **Rectificación de los datos:** si el colegio detecta que algunos de los datos son inexactos, debe rectificarlos lo antes posible y, en cualquier caso, en el plazo de un mes desde la recepción de la solicitud, si la hay.

¿Cómo se tiene que actuar si la persona afectada solicita la rectificación de los datos que considera inexactos a un encargado del tratamiento que actúa por cuenta del colegio?

En el acuerdo de encargo del tratamiento, hay que establecer de forma clara si corresponde al encargado del tratamiento atender y dar respuesta a las solicitudes de los derechos a la autodeterminación informativa, como el derecho de rectificación, o bien establecer expresamente que su única obligación es comunicar al responsable del tratamiento que se ha ejercido un derecho.

En el primer supuesto, el acuerdo tiene que establecer la forma y los plazos para atender o, si procede, dar respuesta a las solicitudes de ejercicio de derechos. En el segundo supuesto, hay que establecer la forma y el plazo en que la solicitud y, si procede, la información correspondiente al ejercicio del derecho, deben comunicarse al responsable del tratamiento.

¿Qué mecanismos de actualización, individualizados o masivos, puede adoptar el responsable del tratamiento?

Sin perjuicio de las rectificaciones que pueda hacer a raíz de las solicitudes de ejercicio del derecho de rectificación, o de las inexactitudes de las cuales tenga conocimiento por otras vías, el colegio puede establecer mecanismos de revisión periódica. Por ejemplo, puede comunicar los datos de que dispone, a fin de que cada persona pueda confirmar si sus datos son correctos y actualizados.

Normativa aplicable: art. 5.1.d) RGPD; art. 4 y 32 LOPDGDD.

7.4 El encargo del tratamiento

7.4.1 La figura del encargado del tratamiento

En algunas ocasiones, el desarrollo de la actividad colegial puede requerir la colaboración con otras entidades en determinados ámbitos o externalizar determinados servicios que impliquen el tratamiento de datos personales. Con respecto a la protección de datos personales, eso debe hacerse mediante la figura del encargado del tratamiento.

El encargado del tratamiento, o encargado, es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trata datos personales por cuenta del responsable del tratamiento.

La figura del encargado permite que los colegios profesionales externalicen servicios y, al mismo tiempo, puedan conservar el control efectivo sobre el tratamiento de los datos personales, con independencia de que todas o algunas de las tareas materiales que implique el tratamiento las lleve a cabo otra persona o entidad. Eso sucede, por ejemplo, cuando un colegio encarga a un tercero la gestión de la destrucción de documentación, la gestión de nóminas, el mantenimiento de equipos informáticos, el alojamiento de información, etc.

En estos casos, cuando el acceso del tercero a los datos personales es necesario para prestar el servicio, y se ha formalizado el encargo del tratamiento, no se considera comunicación de datos.

Hay que tener en cuenta que la normativa de contratos del sector público, en los casos en que es aplicable, establece que tiene la consideración de encargado del tratamiento cualquier contratista que, para ejecutar la prestación, tenga que acceder a datos personales de los cuales sea responsable la entidad que ha adjudicado el contrato.

A la hora de escoger al encargado, el responsable del tratamiento tiene que velar para que reúna las garantías necesarias para llevar a cabo el tratamiento de datos personales. A este

efecto, el RGPD prevé, por ejemplo, que los encargados puedan adherirse a códigos de conducta o certificarse, en el marco de los esquemas de certificación previstos en el mismo RGPD.

7.4.2 Formalización del encargo

La regulación de la relación entre el responsable y el encargado tiene que establecerse a través de un contrato, convenio, acuerdo, o acto jurídico que los vincule. Tiene que constar por escrito, incluido el formato electrónico.

El contrato o acto jurídico debe tener el contenido mínimo siguiente, también cuando el encargo lo formule la norma reguladora de las competencias del órgano:

- El objeto.
- La duración.
- La naturaleza.
- La finalidad del tratamiento.
- El tipo de datos personales.
- Las categorías de personas afectadas.
- Las obligaciones y los derechos del encargado, en particular:
    - Seguir las instrucciones del responsable.
    - Garantizar el respeto al deber de confidencialidad.
    - Tomar todas las medidas de seguridad necesarias para garantizar un nivel de seguridad adecuado al riesgo.
    - Respetar el régimen de subcontratación.
    - Asistir al responsable siempre que sea posible, de acuerdo con la naturaleza del tratamiento y mediante las medidas técnicas y organizativas adecuadas.
    - Ayudar al responsable a garantizar el cumplimiento de las obligaciones de seguridad.
    - Poner a disposición del responsable la información necesaria para demostrar que cumple sus obligaciones y permitir y contribuir a la ejecución de auditorías.
    - A elección del responsable, devolver, suprimir o entregar los datos a otro encargado. En todo caso, el encargado del tratamiento puede conservar los datos bloqueados, mientras se puedan derivar responsabilidades de su relación con el responsable del tratamiento.

Los contratos de encargo formalizados antes de la plena aplicabilidad del RGPD (25 de mayo de 2018) deben adaptarse para que sus cláusulas reflejen todos los contenidos del RGPD, de acuerdo con los criterios siguientes:

- Contratos y acuerdos de encargo con fecha de vencimiento: mantienen su vigencia hasta la fecha de vencimiento que tienen señalada.

- Contratos y acuerdos de encargo con duración indefinida: mantienen la vigencia hasta el 25 de mayo de 2022.

En cualquier caso, durante la vigencia del contrato o acuerdo, cualquiera de las partes puede exigir a la otra la modificación del contrato, para adaptarla a lo que establece el RGPD.

Además, hay que tener en cuenta que, en el ámbito de la contratación del sector público, cuando sea aplicable, los pliegos de cláusulas también tienen que incluir las previsiones siguientes:

- La finalidad para la cual se cederán estos datos.
- La obligación del futuro contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo que establece el último párrafo del apartado 1 del artículo 202 de la LCSP.
- La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la cual ponga de manifiesto dónde estarán ubicados los servidores y desde dónde se prestarán los servicios que están asociados.
- La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere el punto anterior.
- La obligación de los licitadores de indicar en su oferta si tienen previsto subcontratar los servidores o los servicios que están asociados, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica de los subcontratistas.

7.4.3 Obligaciones del encargado del tratamiento

Aparte de las obligaciones mencionadas, establecidas en el contrato o acto jurídico vinculante, el RGPD establece una serie de obligaciones directamente exigibles a los encargados del tratamiento.

Así, el encargado tiene que cumplir las obligaciones siguientes:

- Implantar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.
- Designar a un representante, en caso de que el encargado esté establecido fuera de la Unión Europea.
- Llevar un registro de todas las categorías de actividades de tratamiento efectuadas.
- Nombrar a un delegado de protección de datos, si procede.
- Velar por que los datos personales se traten correctamente.
- Cumplir el régimen aplicable a las transferencias internacionales.

- Cooperar con la autoridad de control.
- Notificar las violaciones de seguridad al responsable del tratamiento.

7.4.4 Subcontratación

El encargado del tratamiento puede subcontratar nuevos encargados, con la autorización previa del responsable. La autorización tiene que ser por escrito y puede ser específica o general.

Si la autorización no concreta el subencargado o se produzcan cambios, antes de hacerlos efectivos el encargado tiene que informar al responsable con el fin de darle la oportunidad de oponerse.

El subencargado debe vincularse con el encargado mediante un contrato o acto jurídico análogo al que tiene que establecerse entre el encargado y el responsable, y está sometido a las mismas obligaciones que el encargado.

Si el subencargado incumple las obligaciones de protección de datos, el encargado inicial sigue siendo plenamente responsable ante el responsable del tratamiento respecto al cumplimiento de las obligaciones del subencargado.

7.4.5 Responsabilidad

Los colegios profesionales tienen, como responsables del tratamiento, un deber de diligencia a la hora de escoger al encargado del tratamiento. Es necesario que escojan uno que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo que establece el RGPD, y que garantice la protección de los derechos de las personas afectadas.

El encargado responde directamente del cumplimiento de las obligaciones que le impone el RGPD. Hay tener en cuenta que el régimen sancionador específico previsto por la LOPDGDD para las entidades del sector público, y en concreto para las corporaciones de derecho público cuando las finalidades del tratamiento se relacionan con el ejercicio de potestades de derecho público, sólo es aplicable al encargado del tratamiento si, vista su naturaleza, está incluida dentro de las entidades que enumera el artículo 77 de la LOPDGDD. En caso contrario, se le debe aplicar el régimen sancionador general, con independencia de la naturaleza de la entidad responsable del tratamiento.

Con respecto a los daños que se hayan producido, corresponde al encargado responder de los daños causados por el tratamiento cuando no haya cumplido con las obligaciones del RGPD dirigidas específicamente al encargado, o haya actuado en contra de las instrucciones del responsable. Cuando exista más de un encargado o cuando el

responsable y el encargado hayan participado conjuntamente en la producción de los daños, hay responsabilidad solidaria entre ellos. Por lo tanto, la persona afectada puede exigir toda la indemnización de cualquiera de ellos, sin perjuicio de la posibilidad de que quien la haya satisfecho pueda reclamar al corresponsable o corresponsables la parte de la indemnización correspondiente.

En cuanto a la responsabilidad asumida por el encargado, si en el momento de determinar las finalidades y los medios del tratamiento un encargado infringe el RGPD, hay que considerarlo responsable con respecto a este tratamiento.

Sobre la figura del encargo del tratamiento se recomienda consultar la Guía sobre el encargado del tratamiento en el RGPD, elaborada por esta Autoridad. También se pueden tener en cuenta las cláusulas contractuales tipo aprobadas por la Comisión Europea mediante la Decisión de ejecución (UE) 2021/915, de 4 de junio de 2021.

¿A fin de que un ente trate datos por cuenta de un colegio profesional, es suficiente que éste le dé ciertas indicaciones o instrucciones?

No. Cuando el ente instrumental accede a datos personales que se tratan bajo la responsabilidad del colegio, tiene que hacerlo contando con el contrato o acto jurídico vinculante, en los términos del artículo 28.3 del RGPD.

¿Un colegio profesional puede facilitar datos de los colegiados a una empresa externa para que lleve a cabo una encuesta para el colegio?

Sí. En este caso, la empresa tendría la condición de encargado del tratamiento, siempre que firme el contrato de encargado con el colegio con el contenido que establece el artículo 28.3 del RGPD.

¿Desde el punto de vista de la normativa de protección de datos, cuáles son los requisitos que debe cumplir el colegio para encargar el cobro de las cuotas de los colegiados a una entidad financiera?

El colegio tiene que escoger una entidad que ofrezca garantías adecuadas con respecto al tratamiento de los datos que el colegio le facilite o que recoja la entidad por cuenta del colegio, y tiene que suscribir un contrato o acuerdo de encargo con esta entidad, con el contenido que establece el artículo 28.3 del RGPD.

¿Quién es el responsable del tratamiento, cuando el colegio profesional encarga la recogida de datos y la elaboración de la guía o lista profesional a una entidad colaboradora?

En este caso, el responsable del tratamiento es el colegio. La entidad colaboradora es una encargada del tratamiento, siempre que se suscriba el contrato o acuerdo de encargo correspondiente.

Normativa aplicable: considerandos 81 y 97 y art. 4.8, 28, 29, 32.1 y 82 RGPD; art. 33, 70, 77 y MA 5ª LOPDGDD; 11 LRJSP; art. 35.1.d), 71.2.d), 116.1, 122.2, 202.1, 215.4 y DA 25ª LCSP.

7.5 El delegado de protección de datos

Todos los colegios profesionales y los consejos de colegios tienen que designar obligatoriamente un delegado de protección de datos (DPD). El resto de entidades dependientes de los colegios profesionales deben designarlo si concurre alguno de los supuestos siguientes:

- Su actividad principal consiste en operaciones de tratamiento que, por su naturaleza, alcance o finalidades, requieren una observación habitual y sistemática de las personas afectadas a gran escala.
- Su actividad principal consiste en el tratamiento a gran escala de categorías especiales de datos o datos relativos a condenas e infracciones penales.

En cualquier caso, los entes dependientes que no estén obligados a ello pueden designarlo de forma voluntaria.

Requisitos necesarios para ser delegado de protección de datos:

- No se establece una titulación específica, ni certificado, aunque se requiere que tenga conocimientos especializados en derecho, sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y un profundo conocimiento del RGPD que le permita identificar los riesgos asociados a las operaciones del tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y las finalidades del tratamiento.
- Conocimientos del sector de la actividad de que se trate. En este caso, conocimientos sobre el ámbito profesional del colegio, la actividad y la organización colegial, las operaciones de tratamiento que se llevan a cabo y los sistemas de información.

El delegado de protección de datos puede ser:

- Interno: personal del colegio profesional o del consejo de colegios.
- Externo: una persona, organización o empresa ajena al colegio, siempre que se acrediten las competencias profesionales a que hace referencia el RGPD, se garantice que no hay ningún conflicto de interés y se formalice un contrato de encargo del tratamiento, a fin de que pueda acceder a la información personal de la cual es responsable el colegio, necesaria para ejercer las funciones del delegado de protección de datos. Si el delegado es una organización, conviene designar a una persona como punto de contacto.

Hay que tener en cuenta que el RGPD ofrece distintas posibilidades para flexibilizar esta exigencia. Así, por ejemplo, un mismo delegado de protección de datos puede asumir, por encargo, esta función respecto de varios colegios; un colegio o consejo de colegios puede prestar este servicio a otros colegios, etc.

Con respecto a la **posición** del delegado de protección de datos, hay que tener en cuenta los aspectos siguientes:

- El responsable o el encargado tienen que garantizar que el delegado de protección de datos participa de manera adecuada y en el momento oportuno en todas las cuestiones relativas a la protección de datos personales.
- El responsable o el encargado deben apoyarle y facilitarle los recursos necesarios para cumplir sus tareas.
- Hay que garantizar la independencia a la hora de ejercer sus funciones. El delegado de protección de datos no está sometido a las instrucciones del responsable o el encargado, ni puede ser sancionado ni destituido por el ejercicio de sus funciones.
- El delegado de protección de datos tiene que rendir cuentas directamente al nivel jerárquico más alto del responsable o del encargado.
- Aunque puede asumir otras tareas, el responsable o el encargado tienen que evitar que eso pueda dar lugar a un conflicto de intereses. Consiguientemente, no se puede designar como delegado de protección de datos a una persona que participe en el proceso de toma de decisiones sobre los tratamientos o en su implementación, en aspectos tan primordiales, como, por ejemplo, la adopción de las medidas de seguridad (como es el caso del responsable de seguridad), o que asuma la representación y defensa de la corporación.
- El delegado de protección de datos debe tener visibilidad suficiente: una vez designado, el nombre y sus datos de contacto se tienen que incluir en el registro de actividades del tratamiento; además, hay que incluir los datos de contacto tanto en la información que se facilita a las personas afectadas como en las respuestas al ejercicio de derechos. También deben publicarse en la página web, a fin de que las personas afectadas puedan contactar con él de manera fácil y directa.
- Su designación, y cualquier cambio que se produzca, debe comunicarse a la Autoridad Catalana de Protección de Datos.

Funciones del delegado de protección de datos:

- Informar y asesorar al responsable o el encargado y los empleados que se ocupan del tratamiento de sus obligaciones en materia de protección de datos.
- Supervisar el cumplimiento de lo que dispone la normativa de protección de datos personales y de las políticas del responsable o del encargado del tratamiento, en materia de protección de datos personales.
- Ofrecer el asesoramiento que se le solicite sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.
- Intervenir en caso de una reclamación presentada por la persona afectada ante el colegio profesional o bien cuando le sea remitida por la Autoridad Catalana de Protección de Datos.

Un colegio profesional ha modificado el registro de actividades de tratamiento, a raíz de los cambios producidos en varios tratamientos. ¿Tiene que avisar a su DPD de estos cambios?

Sí. Teniendo en cuenta lo que dispone el artículo 31.1 de la LOPDGDD, debe comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

¿La obligación de publicar los datos del delegado de protección de datos requiere incluir su nombre?

La obligación de publicar los datos de contacto del delegado de protección de datos puede cumplirse difundiendo un número de teléfono de contacto, una dirección postal y/o una dirección electrónica, sin incluir necesariamente su nombre.No obstante, en el registro de actividades del tratamiento tienen que constar el nombre y apellidos y los datos de contacto.

¿El delegado de protección de datos puede ejercer funciones de responsable de seguridad, o deben ser personas diferentes?

El DPD actúa como interlocutor ante la autoridad de control, hace recomendaciones, informa, asesora y supervisa los tratamientos, entre otros. En cambio, el responsable de seguridad se encarga de implementar las medidas de seguridad necesarias desde una esfera técnica y gestiona los riesgos que se puedan plantear. Previsiblemente, puede haber un conflicto de intereses entre ambas figuras que impide que coincidan en una misma persona.
No obstante, la colaboración entre ambos es imprescindible.

Normativa aplicable: art. 37, 38 y 39 RGPD; art. 34.1.a), 35, 36 y 37 LOPDGDD.

7.6 Las transferencias internacionales de datos

Cuando los colegios profesionales necesitan transferir datos fuera del Espacio Económico Europeo (por ejemplo, porque han contratado como encargada del tratamiento a una empresa fuera de este ámbito, han externalizado determinados servicios en la nube o utilizan determinadas plataformas de servicios, entre otros supuestos), es necesario tener en cuenta que los datos personales sólo se pueden comunicar fuera del Espacio Económico Europeo en los casos siguientes:

- A países, territorios o sectores específicos sobre los cuales la Comisión Europea ha adoptado una decisión que reconoce que ofrecen un nivel de protección adecuado. Se pueden consultar los países con decisión de adecuación en la página web de la Comisión Europea.

- Cuando se han ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino. El responsable o el encargado del tratamiento sólo pueden hacer una transferencia internacional si el destinatario ofrece garantías adecuadas y las personas afectadas cuentan con derechos exigibles y acciones legales efectivas. Estas garantías se pueden ofrecer mediante:
  - Un instrumento jurídicamente vinculante y exigible entre las autoridades o los organismos públicos.
  - Normas corporativas vinculantes.
  - Cláusulas tipo de protección de datos adoptadas por la Comisión Europea.[3]
  - Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión Europea.
  - Un código de conducta aprobado, junto con compromisos vinculantes y exigibles del responsable o del encargado del tratamiento de que en el país tercero se aplican las garantías adecuadas, incluidas las relativas a los derechos de las personas afectadas.
  - Un mecanismo de certificación, junto con compromisos vinculantes y exigibles del responsable o del encargado del tratamiento de que en el país tercero se aplican las garantías adecuadas, incluidas las relativas a los derechos de las personas afectadas.
  - Con la autorización de la Autoridad Catalana de Protección de Datos, si se aportan las garantías adecuadas mediante:
    - Cláusulas contractuales entre el responsable o el encargado y el responsable, el encargado o el destinatario de los datos personales en el tercer país u organización internacional.
    - Disposiciones incorporadas en acuerdos administrativos entre las autoridades o los organismos públicos, que incluyan derechos efectivos y exigibles para las personas interesadas. Esta posibilidad puede ser aplicable a los colegios profesionales, cuando se trate del ejercicio de sus funciones públicas.

- Cuando sea de aplicación alguna de las excepciones siguientes:

[3] Hay que tener en cuenta la Decisión de ejecución de la (UE) 2021/914 de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y el anexo a esta decisión.

a) La persona afectada ha dado explícitamente su consentimiento a la transferencia propuesta, después de haber sido informada de los riesgos de estas transferencias a causa de la ausencia de una decisión de adecuación y de garantías adecuadas.
b) La transferencia es necesaria para ejecutar un contrato entre la persona afectada y el responsable del tratamiento, o para ejecutar medidas precontractuales adoptadas a solicitud de la persona afectada.
c) La transferencia es necesaria para formalizar o ejecutar un contrato entre el responsable del tratamiento y otra persona física o jurídica, en interés de la persona afectada.
d) La transferencia es necesaria por razones importantes de interés público, que tiene que estar reconocido por el derecho de la Unión o de los estados miembros, que se aplica al responsable del tratamiento.
e) La transferencia es necesaria para formular, ejercer o defender reclamaciones.
f) La transferencia es necesaria para proteger derechos vitales de la persona afectada o de otras personas, cuando la persona afectada está física o jurídicamente incapacitada para dar el consentimiento.
g) La transferencia se efectúa desde un registro público que, de conformidad con el derecho de la Unión o de los estados miembros, tiene por objeto facilitar información al público y está abierto a la consulta del público en general o de cualquier persona que acredite un interés legítimo, pero sólo si se cumplen, en cada caso particular, las condiciones que establece el derecho de la Unión o de los estados miembros para hacer la consulta. En este caso, no tiene que abarcar la totalidad de los datos personales ni categorías enteras de datos personales que contiene el registro.

Las excepciones previstas en las letras *a), b)* y *c)* no son aplicables a las actividades desarrolladas por los colegios profesionales en ejercicio de poderes públicos.

- Si no se da ninguna de las condiciones anteriores, la transferencia internacional de datos sólo se puede realizar si se cumplen todas las condiciones siguientes:
  - No es repetitiva.
  - Sólo afecta a un número limitado de personas afectadas.
  - Es necesaria para las finalidades de intereses legítimos imperiosos perseguidos por el responsable del tratamiento.
  - El responsable del tratamiento ha evaluado todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ha ofrecido garantías adecuadas respecto de la protección de datos personales.

Esta posibilidad no es aplicable a las actividades desarrolladas por los colegios profesionales en el ejercicio de sus poderes públicos.

El responsable tiene que informar a la APDCAT de la transferencia. También debe informar a las personas afectadas, así como de los intereses legítimos imperiosos perseguidos.

Normativa aplicable: considerandos 101 a 116 y art. 40, 44 a 50 y 57.*r)* RGPD; art. 40 a 43 LOPDGDD.

7.7 La seguridad de los datos: integridad y confidencialidad

El responsable del tratamiento y el encargado tienen que velar que los datos se traten de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.

Eso hace necesario que el responsable y el encargado garanticen la confidencialidad, la integridad y la disponibilidad de los datos.

Para hacerlo, en primer lugar, hay que identificar y evaluar los riesgos existentes y, a partir de aquí, determinar las medidas de seguridad necesarias con el fin de mitigarlos o, si procede, eliminarlos.

7.7.1 El deber de confidencialidad

El responsable del tratamiento, el encargado y todas las personas que actúen bajo su autoridad están obligados a garantizar la confidencialidad de la información a la cual tengan acceso en ejercicio de sus funciones, a fin de que no sea revelada accidental o voluntariamente a personas no autorizadas, a menos que una ley lo exceptúe.

Este deber conlleva no sólo la imposibilidad de revelar a terceros la información en poder del colegio profesional a la cual se haya accedido en ejercicio de las funciones atribuidas, sino que obliga también a que, dentro del colegio profesional, cada trabajador pueda acceder sólo a la información necesaria para ejercer sus funciones.

A este efecto, el responsable y el encargado tienen que adoptar las medidas técnicas y organizativas necesarias, como la implantación de sistemas de control físico de la información (por ejemplo, cierres de dependencias y armarios), establecer una política y un sistema de asignación de permisos (por ejemplo, acceso mediante claves o certificados), implantar sistemas de control de accesos, etc.

Para garantizar el deber de confidencialidad, se pueden incorporar cláusulas de confidencialidad en los contratos de trabajo y en los protocolos y regulaciones internas. El deber de confidencialidad del personal se extiende incluso después de que haya finalizado la relación laboral.

También hay que incluir las previsiones oportunas en los contratos y acuerdos de encargo del tratamiento que se firmen, para que el encargado firme estas cláusulas con sus trabajadores.

La obligación de confidencialidad prevista en la normativa de protección de datos es complementaria del deber de secreto profesional para determinadas profesiones, de conformidad con su normativa aplicable.

¿El deber de confidencialidad forma parte del secreto profesional?

Aunque están relacionados, no hay que confundirlos. El deber de confidencialidad previsto en la normativa de protección de datos afecta a cualquier persona que intervenga en el tratamiento de los datos personales y es complementaria al deber de secreto profesional a que están sometidas las personas que ejercen determinadas profesiones.

¿Cualquier trabajador de un colegio profesional puede acceder a toda la información sobre terceras personas de que dispone el colegio?

Los trabajadores sólo pueden tener acceso a la información necesaria para ejercer las funciones que tienen atribuidas.

¿Una agrupación de personas colegiadas, constituida en el seno del colegio, puede tener acceso a los datos de los nuevos colegiados para facilitarles información sobre las actividades que lleva a cabo la agrupación?

Dada la información que contiene el registro de colegiados y la información de la guía de colegiados, se puede considerar habilitada la comunicación de los datos relativos a los nuevos colegiados (datos identificativos y de contacto –dirección profesional-, número de colegiación y la fecha de incorporación en el colegio) a la agrupación, sin consentimiento de los afectados.

¿Un miembro de la junta de gobierno de un colegio profesional puede utilizar los datos personales que ha conocido en ejercicio de sus funciones para hacer difusión en un blog personal?

Cualquier uso de la información personal posterior a un acceso legítimo del miembro de la junta de gobierno tiene que estar, igualmente, fundamentado en una finalidad legítima y compatible con la finalidad que justificó el acceso. Si el uso posterior comporta revelar datos personales a terceras personas, como puede ser la publicación de información en un blog sin una base jurídica que lo ampare, podemos estar ante una actuación que no se adecua a la normativa de protección de datos, aunque en origen el acceso se considerara legítimo.

Normativa aplicable: art. 5.1.f) RGPD; 5 LOPDGDD.

7.7.2 La integridad de los datos

Se trata de una exigencia directamente ligada con el principio de exactitud. La información no puede sufrir modificaciones no autorizadas. Así, los datos personales deben tratarse de forma que se garantice la protección contra la alteración, pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.

Normativa aplicable: art. 5.1.*f)* RGPD.

7.7.3 La disponibilidad de los datos

No disponer de la información necesaria para tomar decisiones, aunque sea temporalmente, puede comportar consecuencias para los derechos, libertades e intereses de las personas afectadas. Por eso, es importante que el responsable y el encargado del tratamiento adopten medidas técnicas y organizativas (como las copias de seguridad o soluciones alternativas en caso de fallo del sistema eléctrico, etc.) que aseguren la disponibilidad de la información y los sistemas de información de manera continuada.

Normativa aplicable: art. 5.1.*f)* RGPD.

7.7.4 El análisis de riesgos

El análisis de riesgos es el elemento clave a la hora de determinar las medidas de seguridad a aplicar (técnicas y organizativas), ya que deben ser adecuadas a la probabilidad y la gravedad de los riesgos que se pueden derivar para los derechos y libertades de las personas.

Sin perjuicio de que el análisis de riesgos debe llevarse a cabo antes de iniciar el tratamiento, se trata de una obligación que afecta a toda la vida del tratamiento. Por eso, y dado que los riesgos pueden variar, hay que revisarlo periódicamente y siempre que se produzca algún cambio sustancial en el tratamiento.

Sobre esta cuestión, nos remitimos a lo que ya se ha expuesto en el apartado 6.3 de esta guía

¿Es recomendable utilizar sistemas de mensajería instantánea (SMI), a la luz de las indicaciones de la Resolución 280/XI del Parlamento de Cataluña?

Los colegios profesionales, como responsables de tratar datos de los colegiados y de otros afectados para cumplir sus funciones, tienen que asegurarse de que los terceros prestadores de servicios y de sistemas de comunicación cumplen, a su vez, sus responsabilidades Eso, ya sea como encargados del tratamiento o, si procede, como responsables del tratamiento de los datos de los usuarios (en el caso de los

SMI), dado que el tratamiento está sometido a las exigencias de los principios y garantías de la normativa europea de protección de datos.

Así, cuando consideren la elección de un determinado sistema de mensajería instantánea (SMI) es necesario que lleven a cabo un análisis de los riesgos existentes (probabilidad y gravedad) teniendo en cuenta, especialmente: la finalidad de la comunicación; la información personal que hay que tratar; la existencia de consentimiento libremente otorgado por los afectados; las medidas concretas de seguridad aplicadas por el sistema de mensajería; los mecanismos de certificación; las transferencias internacionales de datos y la ubicación de los servidores; el derecho de información y la transparencia, en atención a las previsiones del RGPD.

7.7.5 Las medidas de seguridad

El RGPD no establece una lista de medidas de seguridad a aplicar. De acuerdo con el análisis de riesgos realizado, el responsable y el encargado del tratamiento tienen que determinar e implementar, caso por caso, las medidas de seguridad apropiadas, en función del riesgo, para garantizar la confidencialidad, la integridad y la disponibilidad de los datos.

Hay que tener en cuenta los aspectos siguientes:

- El estado de la técnica.
- Los costes de aplicación.
- La naturaleza, el alcance, el contexto y las finalidades del tratamiento,
- La probabilidad y la gravedad de los riesgos para los derechos y las libertades de las personas físicas.

Siempre que ejerzan funciones de naturaleza pública, los colegios profesionales y los entes de naturaleza pública y las fundaciones del sector público que dependen de ellos tienen que aplicar, como mínimo, las medidas establecidas en el Esquema Nacional de Seguridad (ENS). En el ejercicio de las funciones privadas la aplicación del ENS no es obligatoria, aunque nada impide que el análisis de riesgos también se pueda llevar a cabo de acuerdo con este esquema.

El resto de las entidades que dependen de los colegios profesionales pueden aplicar también las medidas que se derivan del ENS, u otras, siempre que sean adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales atendiendo a los riesgos existentes. La adhesión a un código de conducta o a un mecanismo de certificación puede servir de elemento para demostrar que se cumple esta obligación.

Cuando se prestan los servicios a través de un encargo del tratamiento, en el contrato o acto jurídico vinculante también hay que asegurar, como mínimo, que se aplican las medidas que corresponde adoptar al responsable.

Las medidas de seguridad aplicadas deben establecerse e implementarse antes de iniciar el tratamiento y deben revisarse periódicamente y siempre que se produzca algún cambio sustancial en el tratamiento o en los riesgos que se derivan.

El responsable y el encargado del tratamiento tienen que tomar medidas para garantizar que cualquier persona que actúa bajo su autoridad y que tiene acceso a datos personales los tratará siguiendo instrucciones del responsable, a no ser que esté obligada en virtud del derecho de la Unión o de los estados miembros.

¿Qué medidas de seguridad tiene que implementar un colegio profesional para proteger los datos personales que trata?

El colegio profesional tiene que implementar cualquier medida que resulte necesaria atendiendo los riesgos que existan. Con respecto a los tratamientos automatizados que lleve a cabo en el ejercicio de potestades de derecho público, eso incluye, como mínimo, las medidas de seguridad que correspondan de las que prevé el Esquema Nacional de Seguridad.

¿Con respecto a las funciones privadas de los colegios profesionales, se puede aplicar el Esquema Nacional de Seguridad para determinar las medidas de seguridad aplicables a los tratamientos automatizados?

Aunque no es obligatorio aplicar el Esquema Nacional de Seguridad a los tratamientos relativos a las funciones privadas de los colegios, constituye uno de los estándares de seguridad que se puede aplicar para determinarlas.

¿Es obligatoria la figura del responsable de seguridad?

Aunque el RGPD no hace referencia al responsable de seguridad, el ENS sí que prevé esta figura de manera diferenciada del responsable de la información y del responsable del servicio.

El responsable de seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información, gestiona los riesgos que se puedan plantear y, entre otros, firma la declaración de aplicabilidad, analiza los informes de auditoría y eleva las conclusiones al responsable para que se adopten las medidas correctoras adecuadas.

¿La prestación de servicios en modalidad de teletrabajo requiere que se adopten medidas de seguridad especiales?

Sí. El teletrabajo comporta un incremento de los riesgos para los datos personales que se tratan. Por eso, es necesario que previamente el colegio establezca las medidas necesarias e informe al personal, con el fin de garantizar que el tratamiento se realizará de manera segura mediante la regulación del régimen de salida de documentos en soporte físico, el hardware y software que se puede utilizar, las condiciones en que debe llevarse a cabo el acceso o comunicación de los datos (cifrado, VPN, etc.), etc.

Sobre esta cuestión, se puede consultar la "Guía rápida para teletrabajar con seguridad" (Consorcio AOC) o las "Normas de ciberseguridad para la prestación de servicios en la modalidad de teletrabajo" de la Agencia de Ciberseguridad de Cataluña.

Normativa aplicable: art. 32 RGPD; art. 77.1.b) y DA 1.ª LOPDGDD; ENS.

7.7.6 La gestión de los incidentes de seguridad

Se considera un incidente o violación de seguridad cualquier violación de la seguridad que ocasiona la destrucción, la pérdida o la alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra manera, o la comunicación o el acceso no autorizados a estos datos.

Cuando se produce un incidente de seguridad, el responsable del tratamiento tiene que actuar, sin dilación indebida, para llevar a cabo las actuaciones siguientes:

- Identificar el incidente, evaluar los riesgos y determinar las medidas a aplicar para minimizarlos o mitigarlos.
- Documentar el incidente de seguridad, incluidos los hechos, los efectos y las medidas correctoras adoptadas.
- Notificar la violación de seguridad a la Autoridad Catalana de Protección de Datos, si procede.
- Comunicar la violación de seguridad a las personas afectadas, si procede.

Notificación de las violaciones de seguridad a la Autoridad Catalana de Protección de Datos

El responsable tiene que notificar la violación de seguridad a la Autoridad Catalana de Protección de Datos sin dilación indebida y, si es posible, en un plazo máximo de 72 horas desde que haya tenido constancia, a menos que sea improbable que constituya un riesgo para los derechos y las libertades de las personas.

Puede considerarse que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de la naturaleza y el alcance. La mera sospecha de que ha habido un fallo o la constatación de que ha sucedido algún tipo de incidente, sin que se conozcan mínimamente las circunstancias, todavía no tendría que dar lugar a la notificación ya que, en la mayoría de los casos, en estas condiciones no se puede determinar hasta qué punto puede existir un riesgo para los derechos y las libertades de las personas afectadas.

En casos de violaciones de seguridad que, por sus características, pueden tener un gran impacto, es recomendable contactar con la Autoridad Catalana de Protección de Datos tan

pronto como haya evidencias de que se ha producido una situación irregular respecto de la seguridad de los datos. Eso, sin perjuicio de que estos primeros contactos se completen con una notificación formal, más completa, dentro del plazo legalmente previsto.

La notificación tiene que incluir, como mínimo:

- La naturaleza de la violación.
- Las categorías de datos y de personas afectadas.
- El nombre y los datos de contacto del delegado de protección de datos o, si no hay, de la persona de contacto.
- Las posibles consecuencias de la violación.
- Las medidas adoptadas por el responsable para solucionar la violación.
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre las personas afectadas.

Cuando la notificación de alguno de estos aspectos no se pueda hacer dentro de las 72 horas, por ejemplo, a causa de la complejidad para determinar completamente el alcance, posteriormente se puede hacer una notificación complementaria, acompañada de una explicación de los motivos que han ocasionado el retraso.

La notificación se puede hacer a través del trámite electrónico disponible en la sede electrónica de la Autoridad Catalana de Protección de Datos.

El encargado del tratamiento debe notificar al responsable del tratamiento, sin dilación indebida, las violaciones de la seguridad de los datos personales de las cuales tenga conocimiento.

Comunicación de las violaciones de seguridad a las personas afectadas

El responsable tiene que comunicar la violación de seguridad a las personas afectadas cuando entrañe un alto riesgo para sus derechos (por ejemplo, si se revela información confidencial como contraseñas, si se difunden datos sensibles de forma masiva o si se pueden producir perjuicios económicos para las personas afectadas).

Hay que comunicarla sin dilaciones indebidas y en un lenguaje claro y sencillo.

El objetivo de esta comunicación es permitir que las personas afectadas puedan tomar medidas para protegerse de las consecuencias de la violación de seguridad, tan pronto como sea posible.

No es obligatorio realizar la comunicación personal en los casos siguientes:

- Si el responsable ha adoptado medidas de protección adecuadas, como que los datos no sean inteligibles por personas no autorizadas.

- Si el responsable ha aplicado medidas posteriores que garantizan que ya no existe la probabilidad de que se concrete el alto riesgo.
- Si supone un esfuerzo desproporcionado. En este caso, hay que optar por una comunicación pública o una medida parecida, que informe a las personas afectadas de modo igualmente efectivo.

Un colegio profesional sufre un robo de ordenadores portátiles -no encriptados- que almacenaban en su disco duro categorías especiales de datos relativos a colegiados (como, por ejemplo, datos de salud) o datos relativos a infracciones disciplinarias. ¿Hay que notificar esta violación de seguridad a la APDCAT?

Sí. El colegio, como responsable del tratamiento de los datos de los colegiados, tiene la obligación de notificar la violación a la Autoridad sin dilación indebida, y en un plazo máximo de 72 horas desde que ha tenido constancia, ya que hay un riesgo de daño para los colegiados.

Un empleado del colegio pierde un dispositivo móvil que contiene datos personales de las personas usuarias de un servicio del colegio, los cuales están encriptados con un algoritmo de tecnología avanzada y la clave de cifrado se mantiene en posesión segura del responsable. ¿Hay que notificar esta violación de seguridad a la APDCAT?

En principio no sería necesario, pero algunas circunstancias pueden hacerlo aconsejable. Así, si el responsable no dispone de una copia de seguridad de los datos encriptados o el tiempo de restauración es significativo, se producirá una violación de disponibilidad, que podría suponer riesgos para las personas y, por lo tanto, podría ser necesario notificarla a la Autoridad. Por otra parte, si más adelante se hace evidente que la clave de cifrado se ha visto comprometida o que el software o algoritmo de cifrado es vulnerable, el riesgo para los derechos y libertades cambiará y, por lo tanto, en este momento puede ser exigible.

Se produce un breve corte de energía de unos minutos de duración en el centro de atención telefónica del colegio, que impide a su personal llamar por teléfono o acceder a sus registros. ¿Hay que notificarlo a la APDCAT?

No. Eso no es una violación de declaración obligatoria, pero sigue siendo un incidente que hay que documentar y registrar en virtud del artículo 33.5 del RGPD.

Un trabajador del colegio envía un correo electrónico a un usuario equivocado, con información relativa a un expediente de justicia gratuita. ¿Hay que notificarlo a la APDCAT?

Sí, en todo caso, dada la información personal que contienen estos tipos de expedientes.

¿Y si el correo electrónico se ha enviado a otro trabajador del mismo colegio, que no tiene permisos para acceder a la información?

Esta circunstancia es, como mínimo, un incidente que hay que documentar y registrar. Ahora bien, para determinar si es una violación de seguridad que hay que notificar, hay que valorar si supone un riesgo para los derechos y libertades,

especialmente atendiendo a la tipología de datos que se hayan trasladado, el número de personas afectadas, las categorías de personas afectadas (menores, discapacidades, trabajadores, etc.), así como los efectos que puede tener sobre los derechos y libertades de las personas.

Normativa aplicable: considerandos 85 y 86 y art. 33 y 34 RGPD; D.A 9ª LOPDGDD.

7.8 La política de protección de datos

Vista la amplitud de los datos recogidos por los colegios profesionales y las consecuencias para los derechos y libertades de las personas que se pueden derivar de los tratamientos que realizan, especialmente en los que tienen más colegiados o pueden tratar información más sensible, conviene que elaboren un documento de política de protección de datos mediante el cual se defina y se dé a conocer de dónde se obtienen, cómo se tratan y cómo se protegen los datos personales que las personas afectadas les faciliten o que el colegio profesional recoja por otras vías.

El RGPD no establece el contenido detallado que debe tener la política de protección de datos. En cualquier caso, entre otros, puede hacer referencia a las cuestiones siguientes:

- Medidas previstas para incorporar la protección de datos en el diseño y la protección de datos por defecto.
- Medidas adoptadas para cumplir con el deber de información a las personas afectadas y para atender sus derechos.
- Asignación de responsabilidades (designación y atribución de responsabilidades del responsable del tratamiento, del delegado de protección de datos, del responsable de seguridad, del responsable del sistema, etc.).
- Las obligaciones del personal.
- Establecimiento de criterios con respecto al tratamiento de datos (por ejemplo, los criterios para determinar los plazos de conservación de la información, criterios sobre los datos que se recogen de las personas que visitan la página web o previsiones relacionadas con las tecnologías que se pueden utilizar y la seguridad de los datos, protocolos de asignación de permisos, de gestión de contraseñas, auditorías, etc.).
- Establecimiento de criterios para la utilización de las TIC por parte del personal al servicio del colegio profesional (hardware, software, teletrabajo, uso del correo electrónico u otros servicios de mensajería, redes sociales, etc.).
- Establecimiento de protocolos para la gestión, notificación y comunicación de las violaciones de seguridad.
- Establecimiento de criterios y protocolos de actuación con respecto a la transparencia de la información pública.
- Adhesión a códigos de conducta y certificaciones, marcas y sellos de que se disponga.

- Instrumentos para hacer transferencias internacionales.
- Medidas para la concienciación y formación del personal.

Corresponde al delegado de protección de datos supervisar la aplicación de la política de protección de datos.

Normativa aplicable: considerando 78 y art. 24.2, 39.1.*b)* RGPD.

7.9 La adopción de otras medidas proactivas

El RGPD establece una serie de obligaciones que tienen que cumplir los responsables y los encargados del tratamiento, a las que nos hemos referido en los apartados precedentes. Pero más allá de eso, y en virtud del principio de responsabilidad proactiva, deben adoptar también cualquier otra medida técnica u organizativa necesaria para garantizar y poder demostrar que el tratamiento es conforme a la normativa de protección de datos.

La promoción o la adhesión a códigos de conducta y la obtención de certificaciones, sellos o marcas pueden ser algunas de estas medidas.

7.9.1 Los códigos de conducta

Un código de conducta es un conjunto de normas que voluntariamente asume una organización o entidad, con el objetivo de facilitar el cumplimiento de una determinada normativa o conseguir un comportamiento ético, en este caso con respecto al tratamiento de los datos personales.

Según el RGPD, los pueden elaborar las asociaciones y otros organismos representativos de categorías de responsables y encargados del tratamiento. La LOPDGDD establece que también los pueden promover, entre otros, las corporaciones de derecho público.

También se pueden adherir a códigos de conducta los responsables o encargados a los que no es de aplicación el RGPD, con el fin de ofrecer las garantías adecuadas en el marco de las transferencias de datos personales a terceros países o a organizaciones internacionales fuera del Espacio Económico Europeo.

Los responsables o los encargados tienen que asumir compromisos vinculantes y exigibles, ya sea por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar estas garantías adecuadas, incluidas las relativas a los derechos de las personas afectadas.

El contenido del código de conducta tiene que especificar la aplicación de la normativa de protección de datos respecto, por ejemplo, a:

- El tratamiento leal y transparente.
- Los intereses legítimos perseguidos por los responsables en contextos específicos.
- La recogida de datos personales.
- La seudonimización de datos personales.
- La información proporcionada a las personas afectadas.
- El ejercicio de los derechos de las personas afectadas.
- La información que se proporciona a los niños y la protección de estos, así como la forma de obtener el consentimiento de los titulares de la potestad parental o de la tutela sobre el niño.
- Las medidas y los procedimientos relativos a las políticas de protección de datos, la protección de datos en el diseño y la protección de datos por defecto, el análisis de riesgos y las medidas para garantizar la seguridad del tratamiento.
- La notificación de violaciones de seguridad a la autoridad de control y la comunicación de estas violaciones a las personas afectadas.
- La transferencia de datos personales a terceros países o a organizaciones internacionales.
- Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos para resolver las controversias entre los responsables del tratamiento y las personas afectadas respecto del tratamiento.

Los colegios, consejos de colegios o asociaciones de colegios que promuevan el código tienen que presentar el proyecto o, si procede, la modificación o ampliación a la Autoridad Catalana de Protección de Datos. La Autoridad tiene que dictaminar si el proyecto de código o la modificación o ampliación es conforme a la normativa vigente y, si procede, aprobarlo, registrarlo y publicarlo, siempre que el código afecte sólo a actividades de tratamiento en un estado miembro.

La Autoridad Catalana de Protección de Datos ofrece su asesoramiento durante la fase de elaboración del proyecto de código, con el fin de facilitar la tramitación posterior.

Normativa aplicable: art. 40 RGPD; 38 y 77.1.*g)* LOPDGDD.

7.9.2 Las certificaciones, sellos y marcas

La finalidad principal de las certificaciones, sellos y marcas es demostrar que los responsables y encargados del tratamiento cumplen el RGPD. Estos instrumentos no limitan las responsabilidades con respecto al cumplimiento del RGPD, pero sirven para evaluar más rápidamente el nivel de protección de datos de productos y servicios. También puede actuar como mecanismo a tener en cuenta a la hora de acreditar que se selecciona un encargado del tratamiento que ofrece garantías adecuadas; también a la hora de hacer transferencias internacionales; o para graduar eventuales sanciones por incumplimiento.

Estos instrumentos pueden proporcionar directrices a los responsables y a los encargados del tratamiento, tanto respecto de la identificación y la mitigación de los riesgos como respecto del cumplimiento del deber de transparencia.

La certificación es voluntaria, tiene que estar disponible a través de un proceso transparente y puede ser expedida al responsable o al encargado del tratamiento por un período máximo de tres años, renovables en las mismas condiciones, siempre que se sigan cumpliendo los requisitos pertinentes. La certificación la puede expedir una autoridad de control o un organismo de certificación acreditado.

Sobre esta cuestión, se recomienda consultar las Directrices 1/2018 del Comité Europeo de Protección de Datos (CEPD), sobre certificación y criterios de certificación de acuerdo con los artículos 42 y 43 del Reglamento 2016/679, disponible en la página web de la APDCAT.

Normativa aplicable: considerandos 77, 100 y art. 42, 43, 57.1.*n)* RGPD; 39 LOPDGDD.

8. Obligaciones del responsable una vez finaliza el tratamiento; la conservación de los datos

El principio de minimización, y su manifestación concretada en el principio de limitación del plazo de conservación, obligan a cesar en el tratamiento y suprimir y bloquear los datos una vez dejan de ser necesarios para la finalidad para la que se recogieron.

8.1 Limitación del plazo de conservación

Los datos tienen que conservarse de modo que sólo se permita la identificación de las personas afectadas durante el tiempo estrictamente necesario para los fines del tratamiento de los datos. Cuando los datos dejen de ser necesarios o pertinentes, hay que suprimirlos.

Únicamente se pueden conservar por un plazo superior si los datos se conservan anonimizados, o bien se conservan con finalidades de archivo en interés público, de investigación científica o histórica o finalidades estadísticas. Eso, siempre que se apliquen medidas técnicas y organizativas adecuadas para proteger los derechos y las libertades de la persona afectada.

No obstante, hay que tener en cuenta que la supresión no equivale a la destrucción, dado que la normativa de protección de datos prevé el deber de bloqueo de los datos suprimidos. Al respecto, nos remitimos al apartado siguiente.

Hay que informar a la persona afectada respecto del plazo de conservación de los datos y, si no es posible concretarlo, se le tiene que informar sobre cuáles son los criterios utilizados para determinarlo.

De acuerdo con la legislación de archivos, aplicable también a las corporaciones de derecho público, los documentos de las administraciones públicas tienen que someterse a una evaluación, que debe determinar el plazo de conservación (atendiendo a su valor cultural, informativo o jurídico) o bien la eliminación, de acuerdo con el procedimiento establecido reglamentariamente.

El plazo de conservación se establece a través de las Tablas de Acceso y Evaluación Documental (TAAD), aprobadas por el Departamento de Cultura a propuesta de la Comisión Nacional de Acceso, Evaluación y Selección Documental (CNAATD). En la página web del Departamento de Cultura se pueden consultar las TAAD aprobadas para las diferentes series documentales evaluadas.

Aunque se trata de una cuestión distinta, porque en este caso sólo se tiene que limitar el tratamiento, pero no suprimir los datos, también hay que tener en cuenta la necesidad de limitar el tiempo de exposición al público, en particular a través de internet, de determinadas informaciones. Así, si se ha establecido un plazo, la información sólo debe permanecer publicada hasta que transcurra este plazo. Si no hay un plazo de exposición establecido, hay que cesar en la publicación cuando se haya alcanzado la finalidad para la cual se publicó.

En el caso de los colegiados, hay que tener en cuenta que para determinados profesionales la normativa aplicable establece un determinado período de conservación mínimo obligatorio, como por ejemplo en el caso de la normativa aplicable a la conservación de la historia clínica. En este caso, puede ser necesario conservar la información incluso más allá de la jubilación o de la muerte de un profesional autónomo. Para hacer frente a estos supuestos de cese de la actividad, y para garantizar la confidencialidad y también la disponibilidad de los datos, puede ser de utilidad que el colegio profesional prevea un servicio de custodia de esta documentación. Este servicio, contratado por el mismo profesional o por sus herederos, implicaría que el colegio fuera responsable de la custodia de los expedientes, como también de la atención de los derechos de las personas afectadas.

¿El colegio tiene que destruir todos los datos de que dispone sobre un colegiado cuando el colegiado se da de baja? ¿Cuánto tiempo tienen que conservar los datos los colegios profesionales?

Los colegios profesionales tienen que conservar la información personal de la cual disponen mientras resulte necesaria para ejercer las funciones que legalmente tienen atribuidas, o sean necesarias para mantener las relaciones jurídicas establecidas con las personas colegiadas. Cuando los datos dejen de ser necesarios, hay que suprimirlos.

Los datos personales deben suprimirse una vez dejan de ser necesarios para la finalidad para la que se recogieron o, si procede, una vez finalizados los plazos de conservación establecidos por la ley o en las tablas de evaluación documental

aprobadas de acuerdo con la Ley 10/2001, de 13 de julio, de archivos y documentos. La supresión conlleva el bloqueo de los datos durante los plazos de prescripción en que se pueda exigir algún tipo de responsabilidad derivada del tratamiento. Cumplido este plazo, que puede variar según la información tratada y las responsabilidades que se pueden generar, hay que proceder a la eliminación efectiva de la información personal.

Los datos sólo se pueden conservar por un plazo superior si se conservan anonimizados, o bien si se conservan con finalidades de archivo en interés público, de investigación científica o histórica o finalidades estadísticas. Eso, siempre que se apliquen medidas técnicas y organizativas adecuadas para proteger los derechos y las libertades de la persona afectada.

¿Se cumple con la obligación de suprimir los datos si la información personal se anonimiza o disocia de forma irreversible?

La anonimización o disociación de un dato, de forma que no se pueda reidentificar al titular, cumple la obligación de supresión, sin perjuicio del deber de bloqueo.

¿Un colegio de médicos puede hacerse cargo de las historias clínicas que eran responsabilidad de un médico colegiado que ha cesado en su actividad?

Sí. En este caso, el colegio profesional es responsable de la custodia de los expedientes, como también de la atención de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de las personas afectadas.

¿Un colegio profesional está legitimado para aceptar la donación de un fondo documental?

De acuerdo con la normativa de archivos, y con la normativa reguladora de colegios profesionales, puede existir suficiente habilitación en normas con rango de ley para que el colegio se pueda hacer cargo de un fondo documental relacionado con sus funciones, sin tener que disponer del consentimiento de los afectados. A partir del marco normativo aplicable y del principio de limitación de finalidad, el colegio, como responsable, tiene que determinar qué datos del fondo documental pueden ser pertinentes, adecuados y limitados al mínimo necesario para la finalidad histórica, estadística o científica prevista y, en consecuencia, cuáles pueden conservarse para posteriores solicitudes de acceso de terceros y cuáles no.

Normativa aplicable: art. 5.1.e), 13 y 14 RGPD; art. 32 LOPDGDD; art. 9 LAD; art. 8 Decreto 13/2008.

8.2 El deber de bloqueo

El responsable del tratamiento está obligado a bloquear los datos cuando los rectifique o los suprima.

Se trata de una figura que no está prevista en el RGPD, pero sí en la LOPDGDD, y que hay que aplicar tanto cuando se suprimen como cuando se rectifican los datos.

El bloqueo consiste en la identificación y la reserva de los datos, con medidas técnicas y organizativas para impedir el tratamiento, incluida la visualización, excepto para ponerlas a disposición de los jueces y tribunales, el ministerio fiscal o las administraciones públicas competentes, en particular de las autoridades de protección de datos, para exigir posibles responsabilidades derivadas del tratamiento y sólo durante el plazo de prescripción de estas responsabilidades. Los datos bloqueados no pueden tratarse con ninguna otra finalidad.

Transcurrido este plazo hay que destruir los datos.

Cuando la configuración del sistema de información no permita el bloqueo o sea necesaria una adaptación que implique un esfuerzo desproporcionado, hay que hacer una copia segura de la información de forma que conste una evidencia digital, o de otra naturaleza, que permita acreditar que la copia es auténtica, la fecha del bloqueo y que los datos no se han manipulado durante este período.

La obligación de bloqueo no es de aplicación:

- A los datos de los sistemas de videovigilancia.
- A los datos incorporados a sistemas de denuncias internas que no se hayan cursado.
- Cuando la Autoridad Catalana de Protección de Datos haya establecido la exención en alguno de estos supuestos:
    - Cuando, por la naturaleza de los datos o por el número elevado de afectados, conservarlas pueda suponer un riesgo elevado para las personas afectadas.
    - Cuando conservar los datos bloqueados puede suponer un esfuerzo desproporcionado para el responsable del tratamiento.

¿Ante el ejercicio de un derecho de supresión, hay que bloquear los datos? ¿Hay que informar del bloqueo a la persona afectada?

Sí. El responsable del tratamiento está obligado a bloquear los datos cuando los rectifique o los suprima, a menos que se trate de datos obtenidos con sistemas de videovigilancia, datos incorporados a sistemas de denuncias internas que no se hayan cursado o si la Autoridad Catalana de Protección de Datos ha establecido la exención, en alguno de los supuestos del artículo 32.5 de la LOPDGDD.

En la resolución del derecho de supresión, conviene informar de que los datos se conservarán bloqueados y que no se podrán tratar para ninguna finalidad, excepto para ponerlos a disposición de los jueces y tribunales, el ministerio fiscal o las administraciones públicas competentes, en particular de las autoridades de protección de datos, para exigir posibles responsabilidades derivadas del tratamiento y sólo durante el plazo de prescripción de estas responsabilidades.

Normativa aplicable: art. 22.3, 24.4 y 32. LOPDGDD.

9. Régimen de responsabilidad

La vulneración del derecho a la protección de datos genera responsabilidades, que se pueden exigir mediante una reclamación o una denuncia ante la APDCAT o mediante una reclamación de responsabilidad por daños ante el colegio profesional o el consejo de colegios responsable o encargado del tratamiento o, si procede, mediante el ejercicio de acciones ante los órganos jurisdiccionales.

En ciertos casos, puede dar lugar también a la exigencia de responsabilidades penales a las personas que hayan cometido algún delito contra los derechos de las personas, en especial delitos contra la intimidad.

9.1 Reclamaciones ante la Autoridad Catalana de Protección de Datos

Se puede reclamar ante la Autoridad Catalana de Protección de Datos para denunciar hechos que constituyan una infracción de la normativa de protección de datos o en casos en que el responsable del tratamiento desatienda los derechos de acceso, rectificación, supresión, oposición y portabilidad, así como el derecho a la limitación del tratamiento y el derecho a no ser objeto de decisiones automatizadas. La reclamación también puede tener por objeto ambas cuestiones a la vez.

La Autoridad Catalana de Protección de Datos tiene que informar a las personas afectadas sobre el curso o el resultado de la reclamación presentada en el plazo de tres meses.

Reclamaciones para denunciar infracciones de la normativa de protección de datos

Cualquier persona puede presentar una reclamación ante la Autoridad Catalana de Protección de Datos para comunicar hechos que pueden ser constitutivos de una infracción de la normativa de protección de datos.

El régimen sancionador previsto en la normativa de protección de datos es aplicable:

- A los responsables de los tratamientos.
- A los encargados de los tratamientos.
- A los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
- A las entidades de certificación.
- A las entidades acreditadas de supervisión de los códigos de conducta.

En cambio, no es aplicable al delegado de protección de datos.

La tipificación de las infracciones y las sanciones está prevista con carácter general en los artículos 83 y 84 del RGPD y en los artículos 71 a 76 de la LOPDGDD.

Las sanciones aplicables deben graduarse de acuerdo con las circunstancias previstas en el artículo 83.2 del RGPD.

Con respecto a los tratamientos de los colegios profesionales relativos al ejercicio de potestades públicas, hay que tener en cuenta que se les aplica el régimen sancionador especial previsto en la LOPDGDD. En virtud de este régimen, si se ha cometido alguna infracción, la Autoridad tiene que dictar una resolución que sancione con una amonestación y, si procede, imponga las medidas a adoptar para que cese la conducta o se corrijan los efectos de la infracción.

En estos casos, hay que notificar la resolución al responsable o al encargado del tratamiento, al órgano del cual dependa jerárquicamente, si procede, y a los reclamantes que tengan la condición de interesado, si procede.

Las actuaciones y las resoluciones sancionadoras que se dicten en relación con el ejercicio de potestades públicas también deben comunicarse al Síndic de Greuges.

Además, la autoridad de protección de datos tiene que proponer la iniciación de actuaciones disciplinarias cuando haya indicios suficientes para hacerlo. En este caso, el procedimiento y las sanciones que tiene que aplicar el colegio profesional son los que establece la legislación sobre régimen disciplinario o sancionador que sea aplicable.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite que hay informes técnicos o recomendaciones para el tratamiento que no se hayan atendido debidamente, como por ejemplo que no se hayan atendido los informes del delegado de protección de datos, hay que incluir en la resolución en que se impone la sanción una amonestación con la denominación del cargo responsable y se tiene que ordenar la publicación en el boletín oficial que corresponda.

A las infracciones cometidas relativas al resto de tratamientos llevados a cabo por el colegio en ejercicio de funciones que no tengan carácter público, así como las cometidas por los encargados del tratamiento de derecho privado que actúan respecto de tratamientos de los que es responsable el colegio, les es de aplicación el régimen sancionador general.

Los plazos de prescripción de las infracciones son los siguientes:

- Para las infracciones consideradas muy graves, tres años.
- Para las infracciones consideradas graves, dos años.
- Para las infracciones consideradas leves, un año.

La prescripción se interrumpe cuando se inicia, con conocimiento del interesado, el procedimiento sancionador. El plazo de prescripción se reinicia si el expediente sancionador está paralizado durante más de seis meses por causas no imputables al presunto infractor.

Los plazos de prescripción de las sanciones son los siguientes:

- Las sanciones por importe igual o inferior a 40.000 euros, al cabo de un año.
- Las sanciones por importe comprendido entre 40.001 y 300.000 euros, al cabo de dos años.
- Las sanciones por importe superior a 300.000 euros, al cabo de tres años.

El plazo de prescripción de las sanciones empieza a contar a partir del día siguiente del día en que la resolución por la que se impone la sanción es ejecutable o haya transcurrido el plazo para recurrirla. Se interrumpe por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, y vuelve a transcurrir si está paralizado durante más de seis meses por causa no imputable al infractor.

Normativa aplicable: art. 83 y 84 RGPD; art. 70 a 78 LOPDGDD; art. 21 en 25 y MA 2ª LACPD.

Reclamaciones ante la desatención de solicitudes de ejercicio de derechos

Además, las personas afectadas pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos cuando se les deniegue, en parte o totalmente, el ejercicio de los derechos de acceso, de rectificación, de supresión, de limitación del tratamiento, de portabilidad o de oposición, o no reciban respuesta.

Para hacerlo, hay que haber ejercido previamente el derecho ante el responsable del fichero y que lo haya denegado, o haya transcurrido el plazo para hacerlo sin que se le haya notificado la respuesta.

La Autoridad, a través de la tramitación de un procedimiento de tutela de derechos, resolverá en el plazo de seis meses si la denegación es procedente o improcedente. Si en el plazo de seis meses la Autoridad no ha notificado la resolución de la reclamación de tutela de derechos, la persona afectada puede considerar que se ha desestimado.

Contra esta resolución o ante la ausencia de resolución en el plazo mencionado, se puede presentar un recurso potestativo de reposición ante la directora de la Autoridad, o directamente recurso contencioso administrativo ante el juzgado contencioso administrativo de Barcelona.

Si se han vulnerado otros derechos o ha habido actuaciones contrarias a la normativa de protección de datos, se puede presentar una denuncia ante la Autoridad.

¿Ante una vulneración del derecho a la protección de datos que haya provocado un daño o perjuicio, la persona afectada puede reclamar simultáneamente ante la APDCAT y por vía judicial?

Sí. La persona afectada puede denunciar la infracción ante la Autoridad Catalana de Protección de Datos, por vía administrativa, y simultánea o posteriormente (teniendo en cuenta los diferentes plazos para hacerlo) también puede presentar demanda por vía judicial, para reclamar la indemnización por daños y perjuicios.

Normativa aplicable: art. 77 RGPD; art. 16 LACPD.

9.2. Reclamaciones ante los órganos jurisdiccionales

Las personas afectadas pueden interponer recurso contencioso administrativo contra una resolución de la Autoridad que los afecte o ante la ausencia de resolución en el plazo de seis meses de una reclamación por la tutela derechos.

Además, cualquier persona afectada también tiene derecho a interponer un recurso contencioso administrativo si la Autoridad Catalana de Protección de Datos no tramita una reclamación o no informa a la persona afectada sobre el curso o el resultado de la reclamación presentada, en el plazo de tres meses.

Normativa aplicable: art. 78 RGPD.

9.3. Indemnización por daños y perjuicios

Cualquier persona que haya sufrido daños y perjuicios, materiales o inmateriales, como consecuencia de una infracción de la normativa sobre protección de datos, tiene derecho a percibir una indemnización del responsable o del encargado del tratamiento.

Si el daño o perjuicio se produce en el marco de las funciones públicas del colegio profesional, la responsabilidad se exige de acuerdo con el régimen de responsabilidad patrimonial previsto a la LRJSP.

Si el daño se produce en el marco del resto de funciones del colegio profesional, la responsabilidad se exige ante los órganos de la jurisdicción ordinaria, es decir, ante los jueces y tribunales competentes en el orden civil.

El encargado únicamente tiene que responder de los daños y perjuicios causados por el tratamiento cuando no haya cumplido las obligaciones de la normativa de protección de datos dirigidas específicamente a los encargados o cuando haya actuado al margen o en contra de las instrucciones legales del responsable.

Cuando más de un responsable o de un encargado del tratamiento, o cuando un responsable y un encargado hayan participado en la misma operación de tratamiento y sean responsables del daño o perjuicio causado, responden solidariamente, sin perjuicio del derecho a reclamar a los otros responsables o encargados la parte que corresponda a su parte de responsabilidad.

¿Las personas afectadas pueden reclamar una indemnización por los daños o las lesiones sufridas como consecuencia del incumplimiento de la normativa de protección de datos?

Sí, pueden ejercer una acción de reclamación de responsabilidad o, si procede, en el caso de las funciones públicas del colegio, una reclamación de responsabilidad patrimonial de acuerdo con la normativa reguladora del régimen de responsabilidad patrimonial de las administraciones públicas, ante el colegio profesional o, si procede, ante los órganos jurisdiccionales.

Normativa aplicable: art. 82 RGPD.

10. Autoridad de control: la Autoridad Catalana de Protección de Datos.

10.1 Naturaleza y objeto

Es el organismo independiente que tiene por objeto garantizar, en el ámbito de las competencias de la Generalitat, los derechos a la protección de datos personales y de acceso a la información vinculada a ellos.

Se regula por la Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, vigente en todo aquello que no se oponga a la ley mencionada.

Se configura como una institución de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines, con plena autonomía orgánica y funcional, que actúa con objetividad y plena independencia de las administraciones públicas en el ejercicio de sus funciones.

La APDCAT vela para que las entidades del sector público de Cataluña que tratan los datos personales de los ciudadanos respeten el derecho a la protección de datos personales, informa a las personas sobre sus derechos, cómo se ejercen y qué pueden hacer si no se respetan, y atiende sus reclamaciones.

Normativa aplicable: art. 1 y 2 LACPD.

10.2 Ámbito de actuación

Los entes que están dentro del ámbito de actuación de la APDCAT son:

- Las instituciones públicas de Cataluña.
- La Administración de la Generalitat.
- Los colegios profesionales.
- Las entidades autónomas, los consorcios y las otras entidades de derecho público vinculadas a la Administración de la Generalitat o a los entes locales, o que dependen de ellos.
- Las entidades de derecho privado que cumplen, como mínimo, uno de los tres requisitos siguientes con relación a la Generalitat, a los entes locales o a los entes que dependen de ellos:
    - Su capital pertenece mayoritariamente a los entes públicos mencionados.
    - Sus ingresos presupuestarios provienen mayoritariamente de los entes públicos mencionados.
    - En sus órganos directivos, los miembros designados por estos entes públicos son mayoría.
- Las otras entidades de derecho privado que prestan servicios públicos por medio de cualquier forma de gestión directa o indirecta, si se trata de ficheros y tratamientos vinculados a la prestación de estos servicios.
- Las universidades públicas y privadas que integran el sistema universitario catalán, y los entes que dependen de él.
- Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalitat o de los colegios profesionales, si se trata de ficheros o tratamientos destinados a ejercer estas funciones y el tratamiento se lleva a cabo en Cataluña.
- Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña.

Por lo tanto, con respecto a los colegios profesionales, los consejos de colegios y los entes u organismos vinculados o dependientes de ellos que ejercen sus funciones exclusivamente en Cataluña, la APDCAT es la autoridad de control competente respecto de los tratamientos que llevan a cabo, ya sea en el ejercicio de las funciones públicas que tienen atribuidas o de otras funciones.

¿La delegación en Cataluña de un colegio de ámbito estatal está incluida en el ámbito de actuación de la Autoridad Catalana de Protección de Datos?

No. El ámbito de actuación de la Autoridad Catalana de Protección de Datos se limita a los colegios y consejos de colegios que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña.

Normativa aplicable: art. 156 EAC; 3 LACPD.

10.3 Organización

La Autoridad dispone de dos órganos:

- El director o directora, que dirige la institución y ejerce su representación.
- El Consejo Asesor de Protección de Datos, órgano de asesoramiento y participación de la Autoridad, constituido por representantes de las diferentes instituciones incluidas en su ámbito de actuación.

Normativa aplicable: art. 6 y s. LACPD; 13 y s. Decreto 48/2003.

10.4 Funciones y potestades

El RGPD atribuye a todas las autoridades de protección de datos las funciones siguientes:

- Controlar y garantizar la aplicación de la normativa de protección de datos.
- Promover la sensibilización y la comprensión del público respecto de los riesgos, las normas, las garantías y los derechos relacionados con el tratamiento. Las actividades dirigidas específicamente a los niños tienen que ser objeto de una atención especial.
- Asesorar, de conformidad con el derecho de los estados miembros, al parlamento nacional, el gobierno y otras instituciones y organismos, sobre las medidas legislativas y administrativas relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento.
- Promover la sensibilización de los responsables y los encargados del tratamiento sobre las obligaciones que les corresponden de acuerdo con la normativa de protección de datos.
- Previa solicitud, facilitar información a cualquier persona afectada sobre el ejercicio de sus derechos y, si procede, cooperar con las autoridades de control de otros estados miembros con esta finalidad.
- Tramitar las reclamaciones presentadas por una persona afectada, por un organismo, una organización o una asociación; asimismo, investigar el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.
- Cooperar con otras autoridades de control, en particular compartiendo información, y prestar asistencia mutua con la finalidad de garantizar la coherencia en la aplicación y la ejecución del RGPD.
- Llevar a cabo investigaciones sobre la aplicación del RGPD, en particular de acuerdo con la información recibida de otra autoridad de control o de otra autoridad pública.

- Hacer un seguimiento de cambios relevantes que tienen incidencia en la protección de datos personales, en particular los relativos al desarrollo de las tecnologías de la información y la comunicación y a las prácticas comerciales.
- Adoptar las cláusulas contractuales tipo para encargados del tratamiento.
- Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos.
- Ofrecer asesoramiento sobre las operaciones de tratamiento sometidas a consulta previa.
- Instar a la elaboración de códigos de conducta y dictaminar y aprobar los códigos de conducta que ofrecen garantías suficientes.
- Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos, y aprobar los criterios de certificación.
- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas.
- Elaborar y publicar los criterios para acreditar a los organismos de supervisión de los códigos de conducta y de los organismos de certificación.
- Acreditar a los organismos de supervisión de los códigos de conducta y los organismos de certificación.
- Autorizar las cláusulas contractuales y las disposiciones a que se refiere el artículo 46, apartado 3, del RGPD.
- Aprobar normas corporativas vinculantes.
- Contribuir a las actividades del Comité Europeo de Protección de Datos.
- Llevar registros internos de las infracciones del RGPD y de las medidas que se han adoptado.
- Llevar a cabo cualquier otra función relacionada con la protección de los datos personales.

Además, la LACPD también establece, entre otras, las funciones siguientes:

- Responder las consultas que formulan las entidades de su ámbito de actuación sobre la protección de datos personales en poder de las administraciones públicas y colaborar con estas entidades, en la difusión de las obligaciones derivadas de la legislación reguladora de estas materias.
- Emitir el informe preceptivo sobre las disposiciones que afectan a la protección de datos personales de la Generalitat. En el caso de los colegios profesionales, este informe es potestativo.
- Elaborar planes de auditoría.

El responsable y el encargado del tratamiento tienen que cooperar con la APDCAT cuando se lo soliciten en ejercicio de sus funciones.

Para ejercer estas funciones, la APDCAT cuenta con las potestades siguientes:

Poderes de investigación:

- Ordenar al responsable y al encargado del tratamiento, y si procede a su representante, que faciliten cualquier información que necesite para cumplir sus funciones.
- Llevar a cabo investigaciones en forma de auditorías de protección de datos.
- Revisar las certificaciones que se expiden en virtud de lo que dispone el artículo 42, apartado 7, del RGPD.
- Notificar al responsable o al encargado del tratamiento las presuntas infracciones de la normativa de protección de datos.
- Obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para ejercer sus funciones.
- Obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluido cualquier equipo y medio de tratamiento de datos, de conformidad con el derecho procesal de la Unión o de los estados miembros.

Poderes correctivos:

- Dirigir a cualquier responsable o encargado del tratamiento una advertencia, si las operaciones de tratamiento previstas pueden infringir lo que dispone la normativa de protección de datos.
- Dirigir a cualquier responsable o encargado del tratamiento una amonestación, si las operaciones de tratamiento han infringido lo que dispone el RGPD.
- Ordenar al responsable o al encargado del tratamiento que atienda las solicitudes de ejercicio de los derechos de la persona afectada, en virtud de lo que dispone el RGPD.
- Ordenar al responsable o el encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del RGPD y la LOPDGDD, de una determinada manera y dentro de un plazo especificado, si procede.
- Ordenar al responsable del tratamiento que comunique a la persona afectada las violaciones de la seguridad de los datos personales.
- Imponer una limitación temporal o definitiva del tratamiento, incluida la prohibición.
- Ordenar la rectificación o la supresión de datos personales o la limitación de tratamiento, y la notificación de estas medidas, a los destinatarios a quienes se han comunicado datos personales.
- Retirar u ordenar al organismo de certificación que retire una certificación emitida, u ordenar al organismo de certificación que no lo emita, si no se cumplen los requisitos para la certificación o si se dejan de cumplir.
- Imponer una multa administrativa, además de las medidas mencionadas en este apartado o en lugar de estas medidas, según las circunstancias de cada caso particular.

- Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Poderes de autorización y consultivos:

- Asesorar al responsable del tratamiento, mediante la consulta previa.
- Emitir, por iniciativa propia o previa solicitud, dictámenes destinados a las entidades incluidas en el ámbito de actuación de la Autoridad, sobre cualquier asunto relacionado con la protección de los datos personales,
- Autorizar el tratamiento cuando se requiera la autorización previa.
- Emitir un dictamen y aprobar proyectos de códigos de conducta.
- Acreditar a los organismos de certificación.
- Expedir certificaciones y aprobar criterios de certificación.
- Adoptar las cláusulas tipo de protección de datos para el encargado del tratamiento.
- Autorizar las cláusulas contractuales mencionadas en el artículo 46.3.*a)* del RGPD.

- Autorizar los acuerdos administrativos que prevé el artículo 46.3.*b)* del RGPD.
- Aprobar normas corporativas vinculantes.

Normativa aplicable: art. 31, 57 y 58 RGPD; art. 5 y 15 y s. LACPD; art. 57 a 62 LOPDGDD.

Abreviaturas

EAC: Estatuto de Autonomía de Cataluña.

EBEP: Texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre.

ENS: Esquema Nacional de Seguridad, aprobado por el Real Decreto 311/2022, de 3 de mayo.

ET: Texto refundido del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre.

Instrucción 1/2009: Instrucción 1/2009 de la Agencia Catalana de Protección de Datos, de 10 de febrero de 2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

LACPD: Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos.

LCSP: Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por el cual se transponen al ordenamiento jurídico español las directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

LEC: Ley 23/1998, de 30 de diciembre, de Estadística de Cataluña.

Ley 7/2006: Ley 7/2006, de 31 de mayo, del ejercicio de profesiones tituladas y de los colegios profesionales.

Ley 2/1974: Ley 2/1974, de 13 de febrero, sobre colegios profesionales.

Ley 2/2007: Ley 2/ 2007, de 15 de marzo, de sociedades profesionales.

Ley orgánica 7/2021: Ley orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

LOPD: Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

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

LOVFCS: Ley Orgánica 4/1997, de 4 de agosto, por la cual se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos.

LRJSP: Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

LT: Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

LTC: Ley 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

RGPD: Reglamento (UE) nº 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE.

RLOPD: Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Anexos

Anexo 1: Modelo de cláusula informativa para documentos de recogida de datos por el colegio profesional.

Anexo 2: Modelo de cláusula informativa para actualizar los datos que aparecen en la lista o guía de personas colegiadas.

Anexo 3: Modelo para ejercer el derecho de acceso.

Anexo 4: Modelo para ejercer el derecho de rectificación y, si procede, el de limitación del tratamiento.

Anexo 5: Modelo para ejercer el derecho de supresión.

Anexo 6: Modelo para ejercer el derecho de oposición y, si procede, el de limitación del tratamiento.

Anexo 7: Modelo para ejercer el derecho de limitación del tratamiento.