Políticas de Seguridad y Protección De Datos

Colegio María Inmaculada Madrid
Hijas de la Caridad
Educación Vicenciana

Colegio Mª Inmaculada Chamberí

Hijas de la Caridad

Paseo General Martínez Campos, 18

28010 MADRID

Índice

1. Objeto y alcance

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución Española. El Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril de 2.016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales suponen la revisión de las bases legales de protección de datos. Para respetar la privacidad en el tratamiento de datos personales en el desarrollo de nuestra actividad, establecemos la siguiente Política de Protección de Datos que será de aplicación a todas las unidades organizativas o departamentos y a todo el personal, propio o ajeno, por tanto todos deberán conocerla y cumplirla.

2. Definiciones

Datos personales: toda información sobre una persona física identificada o identificable (interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, 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 dicha persona.

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

Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Encargado del tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Destinatario: persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, 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.

3. Obligaciones de protección de datos

3.1. Protección de la información de carácter personal

Con el fin de garantizar un nivel de seguridad adecuado al riesgo que para los derechos y las libertades de las personas físicas pueda representar el tratamiento de los datos personales se deben aplicar medidas técnicas y organizativas de seguridad apropiadas.

3.2. Requisitos regulatorios de protección de datos

Los requisitos regulatorios establecidos en el Reglamento General de Protección de Datos son los siguientes:

Respeto a los principios relativos al tratamiento

Principios de licitud, lealtad y transparencia

Cualquier tratamiento o comunicación de datos personales deberá contar con una causa de legitimación.

Además, siempre se debe suministrar al interesado información suficiente, clara e inteligible sobre el tratamiento de sus datos.

Principio de limitación de la finalidad

No se puede realizar ningún tratamiento de datos personales que no responda a una finalidad determinada, explícita y legítima relacionada con nuestra actividad. Una vez recabados los datos para una finalidad no se puede cambiar por otra incompatible sin informar sobre esa nueva finalidad y legitimarla con una base jurídica.

Principio de minimización de datos.

Solo serán objeto de tratamiento los datos estrictamente necesarios de acuerdo con los juicios de proporcionalidad - la finalidad que se persigue no se puede conseguir por otros medios -, idoneidad – el tratamiento puede conseguir el objetivo propuesto - y necesidad - es necesario porque no existe otra medida más moderada para conseguir el propósito con la misma eficacia.

Principio de exactitud.

En la incorporación y registro de los datos personales se debe procurar que sean exactos en y durante el tratamiento se deben mantener actualizados realizando las rectificaciones, de oficio o a instancia del interesado, que procedan.

Principio de limitación del plazo de conservación.

Una vez que los datos han dejado de ser necesarios tanto para la finalidad para la que fueron recabados y para atender las reclamaciones derivadas del tratamiento se deben suprimir.

Principio de integridad y confidencialidad.

Los datos se deben proteger para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes

Principio de responsabilidad proactiva

Se deben adoptar las medidas técnicas y organizativas necesarias para cumplir y poder demostrar el cumplimiento de las normas de protección de datos, a la luz de la evaluación del nivel de riesgo para la protección de datos que se debe realizar.

Adecuada atención a los derechos de las personas

Información al afectado

Sobre el tratamiento de sus datos personales.

Atención diligente al ejercicio por el afectado de sus derechos

De acceso, rectificación y supresión, limitación del tratamiento, portabilidad de los datos, oposición al tratamiento y a las decisiones individuales automatizadas, incluida elaboración de perfiles.

Gestión de los derechos digitales en el ámbito laboral

Desconexión digital y de Intimidad en el uso de dispositivos digitales, de dispositivos de videovigilancia y grabación de sonidos y de sistemas de geolocalización.

4. Organización y responsabilidades en materia de protección de datos.

4.1. Organización

Para la efectiva implantación de la Política de Protección de Datos se requiere:

- Que exista un órgano de coordinación de la protección de datos.
- Que exista un responsable de seguridad que garantice la protección de la información de carácter personal.
- Que las áreas o unidades organizativas que realicen actividades de tratamiento de datos personales para el desarrollo de sus funciones se responsabilicen del cumplimiento de las obligaciones de protección de datos que les incumban.

En consecuencia, se aprueba la siguiente organización:

- Órgano de coordinación de la protección de datos, que será el Delegado de Protección de Datos en caso de ser nombrado o en su defecto, el coordinador de protección de datos.
- Responsable de Seguridad
- Las áreas o unidades organizativas responsables de las actividades de tratamiento de datos personales

Todo el personal deberá atender a los requerimientos que formulen el Coordinador de Protección de Datos o el Responsable de Seguridad en el ejercicio de sus funciones. Todo el personal adscrito a las áreas o unidades funcionales deberá atender a los requerimientos que el responsable formule en el ejercicio de sus funciones relacionadas con la protección de datos. La

falta de atención a los requerimientos sin justa causa podrá ser motivo de responsabilidad.

4.2. Funciones

Órgano de coordinación de la protección de datos

- Informar a la Dirección o Gerencia
- Coordinar y supervisar:
  - Las acciones de adaptación a la normativa de protección de datos.
  - La atención al ejercicio de los derechos por los titulares de los datos.
  - Las posibles brechas de seguridad de los datos personales que se produzcan.
- Mantener actualizado el Registro de Actividades de Tratamiento.
- Realizar evaluaciones del nivel de riesgo por el diseño de nuevas actividades de tratamiento de datos personales o por modificación sustancial de las existentes y proponer las medidas técnicas y organizativas que resulten adecuadas.
- Gestionar y custodiar la documentación relevante de protección de datos.

Responsable de seguridad

- Implantar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad de los datos personales adecuado al riesgo.
- Suministrar la información y documentación que requiera el Órgano de coordinación de la protección de datos y colaborar con dicho Órgano en las acciones que le requiera Área o unidad responsable de actividades de tratamiento.
- Mantener actualizada la información correspondiente a las actividades de tratamiento de las que es responsable.
- Informar a los afectados de las actividades de tratamiento de su responsabilidad.
- Exigir garantías de cumplimiento de la normativa de protección de datos y la firma de contrato de encargo de tratamiento para aquellos servicios que se externalicen e impliquen acceso a datos personales de las actividades de tratamiento de las que es responsable.
- Estar en condiciones de ofrecer garantías de cumplimiento de la normativa de protección de datos cuando se preste un servicio a un tercero que implique acceso a datos personales de la responsabilidad de dicho tercero y suscribir un contrato de encargo de tratamiento.

- Legitimar las comunicaciones o transferencias internacionales de datos personales que se realicen respecto de las actividades de tratamiento de las que es responsable.
- Suprimir los datos personales cuando hayan dejado de ser necesarios para la finalidad para la que se recabaron y hayan transcurrido los plazos de prescripción de las reclamaciones derivadas de tratamiento.
- Suministrar la información y documentación que requiera el Órgano de coordinación de la protección de datos y colaborar con él en las acciones de adaptación a la normativa de protección de datos que le requiera

5. Medidas para cumplir la normativa de protección de datos

Con el fin de garantizar y poder demostrar que los tratamientos de los datos personales que se llevan a cabo son conformes con el Reglamento General de Protección de Datos por cumplir los principios regulatorios y proteger adecuadamente la información de carácter personal se aplicarán las medidas técnicas y organizativas siguientes:

5.1. Antes del tratamiento

Diseño de las actividades de tratamiento de datos personales

Cada nueva actividad de tratamiento de datos personales que se pretenda crear deberá diseñarse identificando la siguiente información:

- La finalidad del tratamiento
- La base jurídica que legitima el tratamiento
- Las categorías de interesados y las categorías de datos
- Las categorías de destinatarios
- Las transferencias de datos personales
- Los plazos previstos para la supresión de las diferentes categorías de datos
- Una descripción de las operaciones de tratamiento y las medidas de seguridad

Por cada nueva actividad de tratamiento que se realice en calidad de encargado del tratamiento por cuenta de un responsable del tratamiento deberá identificarse la siguiente información:

- La identificación del responsable del tratamiento
- Las categorías de tratamientos

- Las transferencias de datos personales
- Una descripción de las operaciones de tratamiento y las medidas de seguridad

Evaluación del nivel de riesgo y determinación de medidas.

Una vez identificadas las operaciones de tratamiento de cada actividad de tratamiento, deberá llevarse a cabo una evaluación del nivel de riesgo y determinar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar el cumplimiento del Reglamento General de Protección de Datos. Si se produjera algún cambio por nuevas tecnologías, uso para finalidades distintas o adicionales o recogida de más datos o datos diferentes, también habría que realizar una evaluación del nivel de riesgo.

Nombramiento del Delegado de Protección de Datos.

Si resultara obligatorio nombrar un Delegado de Protección de Datos o, si no siendo obligatorio, se decidiera su nombramiento voluntario, se le nombrará, se definirán sus funciones, se notificará a la Agencia Española de Protección de Datos y se publicará su nombramiento.

Corresponsabilidad.

Si como consecuencia de la evaluación del nivel de riesgo se llegara a la conclusión de que en alguna de las actividades de tratamiento de datos personales existe corresponsabilidad con otra entidad responsable, se determinarán conjuntamente con dicha entidad los objetivos, los medios de tratamiento y las responsabilidades respectivas.

5.2. Durante el tratamiento

Información al interesado y obtención de su consentimiento

Información sobre el tratamiento

Previamente a la recogida de datos personales se deberá informar al interesado con un lenguaje claro y sencillo y de forma concisa, transparente, inteligible y de fácil de acceso:

- La identificación del responsable del tratamiento
- Los fines del tratamiento
- La base jurídica de legitimación

- Los destinatarios de los datos
- Los derechos del interesado
- Procedencia (cuando los datos no se recaben directamente del interesado)
- Si el interesado está obligado a facilitar sus datos y las consecuencias de no facilitarlos

Siempre se deberá poder acreditar que se ha cumplido la obligación de informar.

Únicamente no será necesario informar cuando el interesado ya disponga de la información o en el caso de que los datos no procedan del interesado, cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado o los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

Obtención del consentimiento

Una de las bases jurídicas de legitimación para el tratamiento de los datos personales es el consentimiento del interesado, que deberá ser inequívoco o explícito, según sea el tipo de tratamiento o la categoría de los datos. Se deberá poder demostrar que se ha obtenido el consentimiento, por tanto deberá conservarse evidencia de su obtención durante todo el tiempo que dure la finalidad del tratamiento.

En cualquier momento se puede retirar el consentimiento tan fácilmente como se le dio. Cuando se ha retirado el consentimiento, todas las operaciones de tratamiento de datos que se basaron en ese consentimiento antes de la retirada son legales.

Atención al ejercicio de los derechos del interesado

Durante todo el tratamiento de los datos personales se deberá garantizar que se atiende adecuadamente y en plazo al ejercicio de cualquier derecho (acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos personales, oposición y decisiones individuales automatizadas).

Para gestionar el ejercicio de los derechos del interesado se deberá cumplir cuanto se establece en el "Procedimiento de atención a los derechos del interesado" aprobado y publicado y llevar al día el "Registro de solicitudes de derechos del interesado".

Mantenimiento de la finalidad y exactitud y actualización de los datos

Una vez obtenidos lícitamente los datos del interesado para una finalidad determinada no puede cambiarse esa finalidad por otra incompatible sin volver a informar y legitimar esa nueva finalidad.

Cuando los datos se obtengan directamente del interesado se presume que son exactos. Para mantener su exactitud, los datos personales objeto de tratamiento deben actualizarse permanentemente, bien sea de oficio o cuando se atienda el ejercicio de un derecho de rectificación o supresión.

Gestión de encargos de tratamiento y servicios sin acceso a datos

En el caso de que para la prestación del servicio el proveedor vaya a necesitar acceder para su tratamiento a datos personales se le considerará encargado del tratamiento, en cuyo caso, se le exigirá, antes de suscribir el contrato de prestación de servicios y acceder a los datos que garantice estar en condiciones de cumplir el Reglamento General de Protección de Datos y una vez garantizado, se le exigirá que suscriba un contrato de encargo de tratamiento Políticas de Seguridad y de Protección de Datos.

En el caso de que para la prestación del servicio el proveedor del servicio no necesite acceder a datos personales de la responsabilidad de la entidad no será necesario exigirle un certificado o una declaración responsable, solamente que suscriba un contrato de confidencialidad.

Seguridad de los datos personales

Para garantizar el nivel de seguridad de los datos se determinarán las medidas de seguridad siguientes:

- Seudonimización y cifrado de datos personales
- Capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento

Asimismo, con periodicidad anual se evaluará y valorará la eficacia de las medidas técnicas y organizativas.

Gestión de brechas de seguridad de los datos personales

Además, cualquier violación de seguridad de los datos personales que se produzca durante el tratamiento se deberá notificar a la Agencia Española de Protección de Datos y, en su caso, además se comunicara a los afectados. Para gestionar y notificar las posibles violaciones de seguridad de los datos personales se deberá cumplir cuanto se establece en el "Procedimiento de gestión y notificación de brechas de seguridad" aprobado y publicado y llevar al día el "Registro de brechas de seguridad".

5.3. Al terminar el tratamiento

Supresión de los datos

Los datos personales no se conservarán más tiempo del necesario para los fines del tratamiento.

Los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la legislación aplicable a fin de proteger los derechos y libertades del interesado.

6. Conocimiento y sensibilización

Toda la documentación de protección de datos relacionada en el apartado anterior será convenientemente publicada para su conocimiento por toda la organización.

Para la correcta comprensión de los principios relativos al tratamiento y de los procedimientos y medidas técnicas y organizativas implantados, se realizarán periódicamente sesiones formativas al personal.