apdcat
Autoritat Catalana de Protecció de Dades

Pautas de protección de datos para los centros educativos

2018

Colección de guías. Num. 3

Generalitat de Catalunya

Índice

El 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante, RGPD), de plena aplicación desde el 25 de mayo de 2018.

Esta nueva regulación, que por primera vez se articula a través de un reglamento europeo, conllevará cambios significativos en la protección de datos de carácter personal, tanto desde el punto de vista de los derechos de las personas como de las obligaciones de las personas y entidades que tratan datos de carácter personal.

1. Objeto

La escuela tiene un papel fundamental en la garantía del derecho de protección de datos personales, no solo como sujeto responsable del adecuado tratamiento de la información de las personas que se relacionan con ella, sino también como elemento esencial en la difusión de este derecho, dado que puede permitir que las personas —los menores—, ya desde el momento de su formación en la escuela, lo conozcan y hagan uso de él.

Este documento pretende prestar el apoyo necesario a los centros educativos (en adelante, las escuelas) para establecer las políticas y los procedimientos necesarios en el tratamiento de datos que deben llevar a cabo en el funcionamiento normal de un centro. Pero, sobre todo, supone una oportunidad para los centros educativos a la hora de revisar sus prácticas en materia de protección de datos y privacidad.

2. La escuela y el RGPD: oportunidad para revisar su cumplimiento

2.1 *Accountability*: principio de responsabilidad proactiva

El responsable del tratamiento, la escuela —en el caso de la escuela pública será el Departamento de Enseñanza de la Generalitat de Catalunya el que deberá establecer si el responsable es cada centro o el propio Departamento—, debe garantizar y poder demostrar que el tratamiento es conforme a la normativa de protección de datos y que ha adoptado las medidas más adecuadas para garantizar los derechos y las libertades de las personas de las que se tratan datos.

Este nuevo principio requiere que la escuela analice qué datos trata, con qué fines lo hace y qué tipo de operaciones de tratamiento lleva a cabo. A partir de este conocimiento detallado, debe valorar el riesgo que puede generar este tratamiento y, de acuerdo con esta valoración, adoptar las medidas pertinentes. Uno de los supuestos que hay que analizar previamente por los riesgos que puede conllevar es el tratamiento de datos de colectivos vulnerables, en el caso de las escuelas, los menores de edad y los menores con necesidades educativas especiales o con discapacidad, entre otros.

Se debe poder demostrar el cumplimiento ante las personas interesadas y ante la autoridad de protección de datos.

Es necesario que la escuela tenga una actitud consciente, diligente y proactiva ante todos los tratamientos de datos personales que lleve a cabo.

2.2 El enfoque al riesgo

Otra novedad de la nueva regulación es que el RGPD adopta un enfoque al riesgo, y que las medidas concretas que se apliquen deben tener en cuenta la naturaleza, el ámbito, el contexto y las finalidades del tratamiento, así como el riesgo para los derechos y las libertades de las personas. Es decir, cada responsable del tratamiento, atendiendo a sus características, adoptará las medidas que corresponda en función de los riesgos existentes.

De acuerdo con este enfoque, algunas de las medidas que el RGPD establece solo se deben aplicar cuando exista un alto riesgo para los derechos y las libertades de las personas, mientras que otras se deben modular de acuerdo con el nivel y el tipo de riesgo que presenten los tratamientos.

La mayoría de los datos tratados en las escuelas son datos de menores de edad. Por ello, dada la vulnerabilidad de este colectivo y las consecuencias que pueden derivarse de un inadecuado tratamiento de su información, tanto en el presente como en el futuro, las escuelas deben extremar, aún más que otros sectores, la diligencia en el tratamiento de esta información.

Estos dos elementos (*accountability* y enfoque al riesgo) se proyectan sobre todas las obligaciones de las organizaciones.

2.3 Protección de datos desde el diseño y por defecto

El Reglamento introduce los conceptos de privacidad desde el diseño y privacidad por defecto. Esto implica que el responsable debe aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas adecuadas, concebidas para aplicar de forma efectiva los principios de protección de datos (por ejemplo, la seudonimización), e integrar las garantías necesarias en el tratamiento para cumplir los requisitos del Reglamento.

Asimismo, el responsable debe aplicar las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo se traten los datos personales necesarios para cada finalidad específica del tratamiento.

Ejemplo

Cuando se diseña una aplicación para uso escolar, en primer lugar debe valorarse cómo afecta a la privacidad del alumnado y se ha de diseñar con el máximo nivel de protección. Es decir, ya desde el diseño, y por defecto, es necesario que se garantice un alto nivel de protección de la privacidad para el alumnado.

3. Tratamiento de datos en las escuelas

3.1 Datos personales

Datos personales cualquier información sobre una persona física identificada o identificable (la persona interesada). Se debe considerar persona física identificable a cualquier persona cuya identidad se pueda determinar directa o indirectamente, en particular, mediante un identificador (este puede ser 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).

Para cumplir con las obligaciones establecidas por la normativa de protección de datos, es necesario identificar los datos que se tratarán y que son susceptibles de protección, así como conocer los conceptos básicos, los principios fundamentales y las obligaciones que permiten garantizar la protección de la información de las personas interesadas o afectadas.

En el caso de los datos del alumnado, el tratamiento de datos en las escuelas se produce por primera vez con la petición de la plaza escolar por parte de los padres, madres y personas tutoras en el proceso de preinscripción y se mantiene, como mínimo, hasta que el alumno finaliza sus estudios en el centro. Esto conlleva el tratamiento de mucha información, ya sea facilitada por la familia, por los profesionales que trabajan en el centro (profesorado, personas tutoras, profesionales de la psicología, etc.) o por el alumnado.

Las escuelas, a fin de ejercer sus funciones, tratan datos de distintos colectivos y de diferentes tipologías. Con carácter previo, conviene analizar si la finalidad perseguida se puede lograr sin necesidad de recoger datos que hagan identificables a personas físicas, ya sea de forma directa o indirecta.

Para poder realizar el «mapa» de los tratamientos de datos, se requiere establecer lo siguiente:

3.1.1 Origen de los datos

- Los datos que recibe la escuela, por ejemplo, cuando el Departamento envía a la escuela la lista de admisiones.
- Los datos que genera la propia escuela, como las notas, los informes psicopedagógicos del alumnado, etc.
- Los datos que la escuela envía, por ejemplo, a proveedores de servicios de la escuela.
- Los datos que se envían al nuevo centro cuando el alumno cambia de escuela, entre otros.

3.1.2 Operaciones o gestiones en las que se tratan datos

- Matriculación y admisión del alumnado: publicidad y contacto con personas interesadas en incorporarse al centro, proceso de preinscripción y matriculación.
- Gestión académica.
- Necesidades educativas especiales.
- Servicios ofrecidos por el centro educativo al alumnado y que completan la finalidad educativa: comedor, transporte escolar, actividades extraescolares, excursiones y colonias, uniformes, etc.
- Gestión del personal docente, administrativo y de servicios.
- Gestión de proveedores.
- Sistemas de pago.
- Plataformas virtuales de enseñanza.
- Sistemas de comunicación y contacto.
- Información médica.
- Servicios a exalumnado.
- Otros.

3.1.3 ¿De quién se tratan los datos?

Persona interesada: persona física identificada o identificable de quien se tratan sus datos.

- Alumnado
- Padres y madres
- Profesorado
- Personas tutoras
- Personal del centro
- Proveedores
- Asistentes a actividades
- Monitores y monitoras
- Exalumnado
- Otras personas con las que se relaciona la escuela

Los datos de carácter personal que las escuelas tratan para desempeñar sus funciones no pertenecen al centro, sino al alumnado, a sus familiares, a su personal o a otras personas físicas con quienes se relacionan. Ellos y ellas son los auténticos titulares de estos datos.

3.1.4 ¿Qué datos se tratan?

Todos los datos que permitan identificar a una persona.

Algunos datos son útiles exclusivamente para identificar a las personas; otros permiten conocer aspectos de su personalidad, evaluar a la persona o conocer aspectos de su historia y circunstancias (estudios, familia, vida laboral, salud, etc.).

- Datos identificativos, como el nombre, la dirección, una fotografía o el DNI.
- Datos de características personales, como lugar de nacimiento, nacionalidad o sexo.
- Datos de circunstancias sociales, como aficiones, estilos de vida o situación familiar.
- Datos académicos y profesionales, como el historial académico y la experiencia profesional.
- Datos económico-financieros, datos bancarios, seguros, subsidios y tarjetas de crédito.
- Datos laborales, como el cuerpo, la categoría, el puesto de trabajo o el historial laboral.
- Datos relativos a la comisión de infracciones penales, como delitos.
- Categorías especiales de datos: datos de salud, ideología, afiliación sindical, religión, creencias, vida sexual u origen racial.

3.1.5 Categorias especiales de datos

El RGPD establece como categorías especiales de datos las que revelen lo siguiente:

- Origen étnico o racial
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación sindical
- Datos de salud
- Vida sexual u orientación sexual de la persona
- Datos genéticos
- Datos biométricos dirigidos a identificar a la persona

El RGPD ha incluido estos dos últimos datos en las categorías especiales de datos:

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física, que proporcionan una información única sobre la fisiología o la salud de esta persona, obtenidos, en particular, del análisis de una muestra biológica.

Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona

física, que permiten o confirman la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, etc.).

Ejemplos de categorias especiales de datos

En las escuelas se tratan habitualmente datos relativos a necesidades educativas especiales y datos de salud del alumnado, como los siguientes:

- Discapacidades físicas, como minusvalías.
- Alergias e intolerancias, para poder organizar el servicio de comedor.
- Psicopedagógicas, para elaborar informes del alumnado.
- Lesiones o enfermedades que pueden tener lugar en la escuela.
- Discapacidades psíquicas, altas capacidades, TDAH, autismos, etc

El tratamiento de este tipo de información requiere un rigor especial en el cumplimiento de los principios de la protección de datos y está sometido a unas condiciones especiales, tanto en lo que respecta a la forma como se debe obtener el consentimiento como a las medidas de seguridad aplicables.

Por ello, se deben establecer los protocolos necesarios para el adecuado tratamiento de esta información, tanto durante el funcionamiento normal del centro (estancia en las aulas, horario de recreo, educación física, comedor, enfermería, evaluación psicopedagógica, etc.) como en situaciones extraordinarias (sustituciones de profesores o personas tutoras, celebraciones de aniversarios, salidas, colonias, etc.).

Cabe recordar que el RGPD prohíbe el tratamiento de este tipo de datos a menos que se den determinadas excepciones que se relacionan en el apartado IV de este documento, titulado ‘Legitimidad’.

3.2 ¿Quién trata los datos personales?

3.2.1 Responsable del tratamiento

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.

En el caso de los centros educativos públicos, nos encontramos ante centros que dependen de un departamento de la Administración de la Generalitat, pero que, a su vez, tienen atribuida cierta autonomía en la gestión. Por ello, el Departamento de Enseñanza de la Generalitat de Catalunya será el que establecerá quién es el responsable del tratamiento.

En el caso de las escuelas concertadas, el responsable del tratamiento será la propia escuela.

3.2.2 Encargado del tratamiento

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

Las escuelas, como responsables de los tratamientos, pueden encargar a terceras personas o a entidades un tratamiento de datos personales o una actividad que comporte el tratamiento de datos de carácter personal, por ejemplo, para organizar:

- Las actividades extraescolares;
- El servicio de autocar;
- El servicio de comedor;
- Otros servicios externalizados (natación, asesoría contable y laboral, destrucción de papel, etc.).

En este caso, hay que tener presente la figura del encargado del tratamiento.

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

El contrato debe establecer, como mínimo, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y las categorías de personas interesadas, así como las obligaciones y los derechos del responsable. El contrato también debe prever, una vez finalizada la prestación de los servicios, el retorno de los datos al responsable del tratamiento o la destrucción de estos.

El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por lo tanto, un deber de diligencia a la hora de escoger al encargado.

Links

Se puede consultar la información necesaria, así como modelos orientativos para formalizar el contrato o acuerdo de encargo de tratamiento, en el siguiente enlace:
Encargado del tratamiento

¿ Qué sucede con los contratos de encargo formalizados antes de la aplicación del RGPD?

Los contratos de encargo formalizados antes de la aplicación del RGPD, en mayo de 2018, deben adaptarse para respetar su contenido. Aunque muchas de las obligaciones derivadas del régimen establecido en el RGPD ya están recogidas en la normativa española, hay que modificar los contratos existentes para que las cláusulas reflejen todos los contenidos del Reglamento, teniendo en cuenta que las remisiones genéricas al artículo del RGPD que los regula no son válidas.

De acuerdo con la disposición transitoria segunda del Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, los contratos y acuerdos de encargo del tratamiento suscritos con anterioridad al 25 de mayo de 2018 mantienen su vigencia hasta la fecha de vencimiento que se señala.

Cuando se trate de encargos con duración indefinida, mantienen su vigencia hasta después de cuatro años, contados desde el 25 de mayo de 2018 (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 establecido en el artículo 28 del RGPD.

3.3 Registro de las actividades de tratamiento de datos (RAT)

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, 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, cotejo o interconexión, limitación, supresión o destrucción.

Cabe recordar que el RGPD suprime, desde el 25 de mayo de 2018, la necesidad de crear formalmente ficheros y notificarlos al registro de protección de datos de las autoridades de control.

3.3.1 Registro de las actividades de tratamiento de datos (RAT)

Los responsables o encargados del tratamiento deben elaborar un registro de las actividades del tratamiento que lleven a cabo.

El RGPD prevé determinadas excepciones a la elaboración de este registro, entre las que no cabrían los tratamientos de datos efectuados por las escuelas.

Este es un instrumento fundamental no solo para la posible supervisión de la autoridad, sino también para disponer de una imagen actualizada de los tratamientos existentes en la escuela, esencial para la gestión de riesgos. El registro debe ser por escrito, incluido el formato electrónico, y se presentará a petición de la autoridad.

3.3.2 ¿Cómo se debe organizar el registro de operaciones de tratamiento?

El registro se puede organizar en torno a operaciones de tratamiento concretas, vinculadas a una finalidad básica común de todas ellas (por ejemplo, gestión académica o gestión de recursos humanos y nóminas), o bien de acuerdo con otros criterios.

Links

La Autoridad Catalana de Protección de Datos (APDCAT) ha desarrollado una sencilla aplicación para llevar el registro de actividades del tratamiento, con el fin de ayudar a los responsables en su gestión. Se puede descargar en el siguiente enlace:
Aplicación para gestionar el registro de las actividades de tratamiento

4. Legitimidad. ¿Cuándo podemos tratar los datos personales?

4.1 Principios. Cómo cumplir con el RGPD

Los tratamientos de datos se deben llevar a cabo respetando, en todo momento, los principios establecidos por el RGPD. Anteriormente ya se ha expuesto uno de los principios que supone una importante novedad en esta regulación, el principio de responsabilidad proactiva.

4.1.1 Licitud, leadtad y transparencia

Los datos se deben tratar con licitud, lealtad y transparencia.

Así, por ejemplo, la escuela debe facilitar a las personas interesadas la información sobre el tratamiento con suficiente antelación, de acuerdo con los plazos máximos establecidos. Asimismo, cuando se introduzcan cambios en el tratamiento de los datos, los comunicará a las personas interesadas y deberá explicarles cómo les afectarán.

4.1.2 Limitación de la finalidad

Los datos se recogerán con determinadas finalidades, explícitas y legítimas, y posteriormente no se deberán tratar de forma incompatible con dichas finalidades. El tratamiento posterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considera incompatible con las finalidades iniciales.

En este sentido, la propia Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE) establece que la información que recojan las escuelas en ejercicio de su función educativa debe ser la estrictamente necesaria para la función docente y orientadora, y no se puede tratar con finalidades distintas de la educativa sin consentimiento expreso.

4.1.3 Minimización de los datos

Los datos deben ser adecuados, pertinentes y deben limitarse a lo que sea necesario en relación con los fines para los que se tratan.

Deben revisarse cuidadosamente los datos que se pretende recoger, para que solo se recojan los que, de acuerdo con este principio, sean necesarios para la consecución de la finalidad perseguida.

4.1.4 Exactitud

Los datos deben ser exactos y, en caso necesario, deben estar actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan.

La falta de actualización de los datos personales puede afectar a la propia gestión académica o, incluso puede conllevar la revelación indebida de datos a terceras personas (por ejemplo, si la dirección no está actualizada o si la escuela no ha registrado debidamente la comunicación de los padres y madres sobre cambios que afectan al régimen legal de patria potestad o guarda y custodia sobre menores).

4.1.5 Limitación del plazo de conservación

Los datos se conservarán de forma que se permita la identificación de las personas interesadas durante el tiempo estrictamente necesario para los fines del tratamiento de datos personales. Los datos se pueden conservar durante periodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, ya sea para la investigación científica o histórica o para fines estadísticos, sin perjuicio de la aplicación de

las medidas técnicas y organizativas adecuadas que impone la normativa de protección de datos con el fin de proteger los derechos y las libertades de la persona interesada.

4.1.6 Integridad y confidencialidad

Los datos deben tratarse de forma que se garantice una seguridad adecuada de estos, 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 apropiadas, tal y como se señala en el apartado "IX".

4.2 Transparencia de la información

La escuela debe ser transparente respecto a los tratamientos de datos que se quieren llevar a cabo, con independencia de que sea necesario obtener el consentimiento de la persona interesada o se cuente con otra base jurídica.

Por ello, en todos los tratamientos que la escuela realice, deberá aplicarse la máxima transparencia, de forma que las personas conozcan en todo momento el uso que se está haciendo de sus datos. Así, por ejemplo, disponer de un aviso de privacidad en las páginas web de las entidades claramente visible permitirá a las personas estar informadas en todo momento.

4.2.1 Información a la persona interesada

La transparencia en el tratamiento de los datos se concreta de forma muy clara en el derecho de información que tiene la persona interesada tanto si los datos se recogen directamente como a través de terceros.

Cuando los datos se recogen directamente de la persona interesada

La información a la persona interesada se puede facilitar adoptando un modelo de información por capas o niveles: se ofrece, en un primer nivel, la información básica y se facilita una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.

Esto se concreta del siguiente modo:

Primer nivel. Información básica que permita tener un conocimiento general del tratamiento.

- La identidad del responsable del tratamiento.
- La finalidad del tratamiento.

- La posibilidad de ejercer los derechos de autodeterminación informativa, el derecho de acceso, rectificación, supresión y oposición, así como el derecho a la limitación del tratamiento, la portabilidad de los datos o a impugnar valoraciones

Segundo nivel. Resto de la información.

- La identidad y los datos de contacto del responsable y, en su caso, 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 los que se fundamenta el tratamiento, si procede.
- Los destinatarios o categorías de destinatarios de los datos.
- La intención de transferir los datos a un tercer país o a una organización internacional y la base para llevarlo a cabo, si procede.
- El plazo durante el cual se conservarán los datos, o los criterios para su determinación.
- El derecho a solicitar el acceso a los datos, la rectificación o la supresión de los datos, la limitación y la oposición al tratamiento y la portabilidad de los datos.
- El derecho a retirar en cualquier momento el consentimiento que se haya prestado.
- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato, y si la persona interesada está obligada a facilitar los datos y las consecuencias de no facilitarlos.
- 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.

Cuando los datos no se recogen directamente de la persona interesada

Además de los aspectos que se acaban de mencionar, se debe indicar:

- Las categorías de datos personales tratados.
- La fuente de la que proceden los datos y si son fuentes de acceso público.

4.2.2 Excepciones al derecho de información

No es necesario informar cuando:

- Los datos se recogen de la persona interesada y la persona interesada ya dispone de la información.
- Los datos no se recogen de la persona interesada y concurre alguna de las siguientes circunstancias:

- La persona interesada ya dispone de toda la información legalmente exigible.
- La comunicación resulta imposible o supone un esfuerzo desproporcionado.
- La obtención o la comunicación está expresamente establecida por el Derecho de la Unión Europea o de los Estados miembros.
- Los datos deben seguir teniendo carácter confidencial por una obligación legal de secreto profesional, incluida una obligación de secreto de naturaleza estatutaria.

4.2.3 ¿Dónde y cómo se debe informar?

La obligación de informar se debe cumplir sin necesidad de requerimiento y el responsable debe poder acreditar con posterioridad que la ha cumplido.

En cualquier caso, la información a las personas interesadas se proporcionará:

- En un lenguaje claro y sencillo.
- De forma concisa, transparente, inteligible y de fácil acceso.
- Equilibrando la concisión y precisión, evitando circunloquios, explicaciones innecesarias o detalles confusos.
- Evitando el abuso de citas legales innecesarias y de términos ambiguos o con escaso sentido para las personas destinatarias.
- Mediante un lenguaje adecuado a su nivel de comprensión, en caso de que los destinatarios sean menores.

Si lo solicita la persona interesada, la información también se puede facilitar verbalmente.

4.2.4 ¿En qué momento del tratamiento se debe dar la información?

La información se debe poner a disposición de las personas interesadas en el siguiente plazo:

- Si la información se obtiene de la propia persona interesada, en el momento en que se solicitan los datos.
- Si la información no se obtiene la propia persona interesada, en un plazo razonable, pero en cualquier caso en el plazo de un mes, salvo cuando sea necesario facilitar la información con anterioridad, por concurrir alguna de las siguientes causas:
  - Si los datos se deben utilizar para comunicarse con la persona interesada, es necesario informarle de ello anteriormente o en la primera comunicación con esta persona.
  - Si está previsto comunicarlos a otro destinatario, es necesario informar de ello anteriormente o en el momento de esta comunicación.

- Si posteriormente se pretende utilizar los datos para una finalidad distinta de aquella para la que se recogieron, se debe proporcionar previamente la información necesaria vinculada a esta nueva finalidad.

Links

En la web de la APDCAT se encuentra disponible la Guía para el cumplimiento del deber de informar, que ofrece directrices y orientaciones para cumplir con esta obligación: Guía para el cumplimiento del deber de informar

¿Se requiere volver a informar a las personas afectadas que ya lo habían estado de acuerdo con la LOPD, para ponerlas al corriente de los nuevos aspectos que exigen los artículos 13 y 14 del RGPD?

El RGPD amplía las cuestiones sobre las que hay que informar a las personas afectadas y modifica algunos aspectos de la forma en que se debe proporcionar esta información. Sin embargo, con respecto a los datos recogidos antes del 25 de mayo de 2018, no es preceptivo informar nuevamente con los requisitos establecidos en el RGPD. La obligación de informar según lo establecido en el RGPD es exigible solo para los datos recogidos después de esta fecha. Sin embargo, si las circunstancias lo permiten, se recomienda aprovechar los actos de comunicación con las personas afectadas para informarlas de los nuevos aspectos que establece el RGPD.

4.3 Bases jurídicas para tratar datos personales

Las escuelas, para ejercer sus funciones, deben tratar un gran volumen de datos personales. El tratamiento solo es lícito si se cumple, al menos, una de las condiciones que se detallan a continuación:

- Cuando la persona interesada ha dado su consentimiento.
- Cuando es necesario para ejecutar un contrato o aplicar medidas precontractuales.
- Para cumplir una obligación legal.
- Para proteger intereses vitales de la persona interesada o de otra persona física.
- Para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- 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 interesada que requieren la protección de datos personales, especialmente si persona interesada es menor. (El contenido de este párrafo no se aplica al tratamiento por parte de las autoridades públicas en el ejercicio de sus funciones).

Para el caso de las categorías especiales de datos, no se permite su tratamiento, salvo si concurre alguna de las circunstancias establecidas en el RGPD, como las siguientes:

- La persona interesada ha dado su consentimiento explícito para el tratamiento de estos datos personales para una o más de las finalidades especificadas.
- El tratamiento es necesario para proteger intereses vitales de la persona interesada o de otra persona física, en el supuesto de que la persona interesada no esté capacitada física o jurídicamente para dar su consentimiento.
- Otras circunstancias, por ejemplo, cuando el tratamiento se refiere a datos personales que la persona interesada ha hecho manifiestamente públicos, cuando es necesario para fines de medicina preventiva o laboral, etc.

Cualquier tratamiento de datos, por tanto, también la comunicación de datos a terceros, debe sustentarse en alguna de las bases jurídicas anteriores.

Algunos ejemplos de comunicaciones pueden ser:

- Comunicaciones de datos para fines académicos.
- Comunicaciones extraacadémicas.
- Comunicaciones con fines administrativos.
- Comunicaciones a administraciones públicas.

4.3.1 LOE: habilitación para el tratamiento de datos en las escuelas

Las escuelas, ya sean de titularidad pública o privada, pueden tratar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa y orientadora. Así lo establece la LOE, que habilita el tratamiento de los datos del alumnado con este fin desde el momento en que el alumno se incorpora a la escuela. La LOE también habilita a la escuela, en su caso, para que ceda datos del alumnado; por ejemplo, datos procedentes del centro donde haya estado escolarizado anteriormente y que se envíen al nuevo centro donde el alumno siga sus estudios.

Asimismo, la LOE habilita a las escuelas para el tratamiento de datos de categorías especiales cuyo conocimiento sea necesario para la educación y la orientación del alumnado.

Para todas aquellas otras funciones que no formen parte de la función docente y orientadora de los centros, será necesario contar con la base jurídica para tratar los datos correspondientes (consentimiento, contrato, interés público, etc.).

4.3.2 Relación Contractual. Habilitación del profesorado y personal de los centros

En cuanto a los datos relativos a su personal, las escuelas pueden tratar los datos de su personal sin necesidad de su consentimiento, cuando se trata de datos necesarios para mantener o cumplir la relación laboral o administrativa que mantengan con el centro.

4.3.3 Consentimiento: Servicios distintos de la función docente y orientadora

Para otros casos en que se necesite tratar los datos con finalidades distintas a la función docente y orientadora, como la publicación de fotografías en la web de la escuela, o la entrega de datos a casas de colonias, museos u otros establecimientos que se visiten, se requiere el consentimiento del titular de los datos, o de su representante en caso de los menores.

El consentimiento debe ser una manifestación de voluntad por la que la persona interesada acepta el tratamiento de sus datos personales, ya sea mediante una declaración o una clara acción afirmativa. Esta manifestación de voluntad debe ser:

- **Libre.** La persona debe tener la posibilidad de rechazar libremente que se traten sus datos.
- **Específica.** El consentimiento se refiere a tratamientos concretos y para una finalidad determinada, explícita y legítima del responsable del tratamiento, sin que se puedan establecer habilitaciones genéricas.
- **Informada.** Es necesario informar a las personas interesadas para que, con antelación al tratamiento, puedan conocer la existencia y los fines de este.
- **Inequívoca.** La solicitud y el otorgamiento del consentimiento deben producirse de forma clara.

El RGPD requiere que la persona interesada preste el consentimiento mediante una declaración inequívoca o una acción afirmativa clara para cada una de las finalidades para las que se solicita el consentimiento. Así, a efectos del RGPD, las casillas ya marcadas, el consentimiento tácito o la inacción no constituyen un consentimiento válido.

Corresponde al responsable del tratamiento la prueba de la obtención del consentimiento de la persona interesada para un tratamiento específico.

¿Se pueden seguir llevando a cabo los tratamientos basados en el consentimiento tácito iniciados antes del 25 de mayo de 2018?

El RGPD establece que el consentimiento debe consistir en una declaración o un acto afirmativo claro, que refleje una manifestación de voluntad libre, específica, informada e inequívoca de la persona interesada de aceptar el tratamiento de datos de carácter personal que le afectan. Por lo tanto, el silencio, las casillas ya marcadas o la inacción

(como, por ejemplo, el consentimiento tácito) no constituyen un consentimiento válido de acuerdo con el RGPD.

De acuerdo con ello, los tratamientos de datos iniciados antes del 25 de mayo de 2018 basados en un consentimiento tácito deben ajustarse a los requisitos del RGPD antes de esta fecha, ya sea mediante la obtención de un nuevo consentimiento que reúna los requisitos establecidos por el RGPD, ya sea mediante alguna otra de las bases jurídicas establecidas por el RGPD.

4.3.4 Consentimiento: Menores de edad

Las escuelas normalmente tratarán datos de menores de edad. Para los tratamientos que requieran consentimiento, es decir, los no incluidos en la función docente y orientadora de los centros, será necesario el consentimiento de los padres, madres o personas tutoras cuando el alumnado sea menor de 14 años.

El alumnado mayor de 14 años podrá consentir por sí mismo, con la excepción de aquellos supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela.

La protección de los menores se concreta, además, en la exigencia de que la información que se les proporciona sea en un lenguaje que les resulte fácilmente comprensible.

4.3.5 Consentimiento: Redes y menores

La escuela debe ser consciente de su responsabilidad en un uso o una difusión inapropiados de las imágenes de los menores. La normativa de protección de datos regula especialmente la protección de los menores en internet, y establece que la utilización y la difusión de imágenes e información personales de los menores en las redes sociales que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del ministerio fiscal, que podrá instar las medidas cautelares y de protección que determine la ley.

Las escuelas, así como cualquier persona que lleve a cabo actividades donde participen menores de edad y donde se traten sus datos (imágenes, voz, etc.), deben garantizar la protección del interés superior del menor y de sus derechos y libertades fundamentales. En este caso, especialmente el derecho a la protección de datos personales, en el momento de la publicación o la difusión de sus datos personales a través de los servicios de la sociedad de la información.

La escuela deberá contar con el consentimiento de los menores o de sus padres, madres o personas tutoras antes de llevar a cabo cualquier publicación o difusión de los datos del alumnado en la web de la escuela o en la intranet de la escuela.

4.3.6 Revocación del consentimiento

La persona afectada puede revocar el consentimiento otorgado en cualquier momento, sin efectos retroactivos. Antes de dar su consentimiento, se deberá informar a la persona interesada de esta posibilidad. Debe ser tan fácil retirar el consentimiento como otorgarlo.

5. Derechos de la persona interesada

5.1 Derechos de la autodeterminación informativa

Estos derechos son personalísimos y los debe ejercer la propia persona interesada o un tercero por representación, ante el responsable del tratamiento.

Los titulares de la patria potestad podrán ejercer siempre estos derechos, en nombre y representación de menores de 14 años.

5.1.1 Derecho de acceso

La persona interesada tiene derecho a saber si el responsable del tratamiento trata datos personales suyos. De ser así, tiene derecho a acceder a la siguiente información, así como a obtenerla:

- Las finalidades del tratamiento, las categorías de datos personales que se tratan y los destinatarios o las categorías de destinatarios a los que se han comunicado o se comunicarán los datos.
- El plazo previsto de conservación de los datos personales o los criterios utilizados para su determinación.
- El derecho a solicitar al responsable del tratamiento la rectificación o supresión de los datos, la limitación del tratamiento o el derecho a oponerse a ellos.
- 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 interesada.
- 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.

La persona interesada tiene derecho a obtener una copia gratuita de los datos objeto del tratamiento. Para copias posteriores, se puede establecer un canon según los costes administrativos. Si se solicita por medios electrónicos, la persona interesada tiene derecho a recibir la información en este mismo formato.

Si las solicitudes son manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento puede cobrar un canon razonable, de acuerdo con los costes administrativos que se han afrontado para facilitar la información o la comunicación, o para llevar a cabo la actuación solicitada, o bien negarse a actuar respecto a la solicitud. El responsable del tratamiento es quien deberá demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

5.1.2 Derecho de rectificación

La persona interesada tiene derecho a rectificar sus datos personales inexactos y a que se completen sus datos personales incompletos, incluso mediante una declaración adicional.

Es necesario que la persona interesada indique de forma clara y detallada lo que se solicita, a qué datos se refiere y qué corrección se debe efectuar. La solicitud debe ir acompañada de la documentación que justifica la rectificación, en su caso.

El responsable deberá comunicar la rectificación a cada uno de los destinatarios, a menos que sea imposible o exija esfuerzos desproporcionados. Si la persona interesada lo solicita, el responsable debe identificar a los destinatarios.

5.1.3 Derecho de supresión o derecho al olvido

Las personas interesadas tienen derecho a obtener la supresión de sus datos (lo que se conoce como derecho al olvido) cuando:

- Los datos ya no son necesarios para la finalidad para la que se recogieron.
- Se revoca el consentimiento en el que se basaba el tratamiento.
- La persona interesada se opone al tratamiento.
- Los datos se han tratado ilícitamente.
- Los datos se deben suprimir 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.

Cuando el responsable ha hecho públicos los datos personales y deben suprimirse, debe adoptar medidas razonables para informar de la supresión a los responsables que están tratando los datos.

El responsable comunicará la supresión a cada uno de los destinatarios, a menos que sea imposible o exija esfuerzos desproporcionados. Si la persona interesada lo solicita, el responsable debe identificar a los destinatarios.

Se prevén algunas excepciones al ejercicio de este derecho:

- El ejercicio del derecho a la libertad de expresión e información.
- El cumplimiento de una obligación legal.
- La existencia de fines de archivo en interés público, de investigación científica o histórica o fines estadísticos.
- La formulación, el ejercicio o la defensa de reclamaciones.

5.1.4 Derecho a la limitación del tratamiento

La limitación de tratamiento supone que, a petición de la persona interesada, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

La limitación se puede solicitar cuando:

- La persona interesada ha ejercido los derechos de rectificación u oposición y mientras el responsable determina, en su caso, atender la solicitud.
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero la persona interesada se opone.
- Los datos ya no son necesarios para el tratamiento, lo que nuevamente determinaría su borrado, pero la persona interesada solicita la limitación porque los necesita para formular, ejercer o defender reclamaciones.

Mientras dure la limitación, el responsable solo puede tratar los datos afectados, más allá de conservarlos, en los siguientes casos:

- Con el consentimiento de la persona interesada.
- Para formular, ejercer o defender reclamaciones.
- Para proteger los derechos de otra persona física o jurídica.
- Por razones de interés público importante de la Unión Europea o de un Estado miembro.

El responsable comunicará la limitación a cada uno de los destinatarios, a menos que sea imposible o exija esfuerzos desproporcionados. Si la persona interesada lo solicita, el responsable debe identificar a los destinatarios.

5.1.5 Derecho a la portabilidad de los datos

El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso por la que la persona interesada tiene derecho a recibir los datos personales que le afectan en un formato estructurado, de uso común y de lectura mecánica, si se cumplen los siguientes requisitos:

- El tratamiento está basado en el consentimiento o en un contrato.

- El tratamiento se lleva a cabo por medios automatizados.

La persona interesada puede solicitar al responsable los datos que ha proporcionado y que le afectan, incluidos los datos derivados de la actividad de la persona interesada.

El derecho a la portabilidad de datos incluye el derecho a que estos se transmitan directamente de responsable a responsable, si es técnicamente posible.

No se puede ejercer este derecho cuando el tratamiento se fundamenta en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

5.1.6 Derecho de oposición

La persona interesada tiene derecho a oponerse al tratamiento de sus datos personales:

- Cuando el tratamiento se basa en el interés público o en el ejercicio de poderes públicos conferidos al responsable, o bien en el interés legítimo perseguido por el responsable del tratamiento o por un tercero. En este caso, la oposición debe fundamentarse en motivos relacionados con su situación personal. El responsable del tratamiento debe dejar de tratarlos, salvo cuando el responsable acredite un interés legítimo imperioso que prevalezca sobre el de la persona interesada o sea necesario para ejercer o defender reclamaciones.
- 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.
- Cuando el tratamiento tiene por objeto el marketing directo, incluida la elaboración de perfiles relacionados con este marketing. En este caso, la persona interesada podrá oponerse al tratamiento de sus datos en cualquier momento, sin necesidad de fundamentar su petición.

5.1.7 Derecho a no ser objeto de decisiones individuales automatizadas

La persona interesada tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre él o que le afecte significativamente, salvo cuando la decisión:

- Sea necesaria para formalizar o ejecutar un contrato entre la persona interesada y un responsable del tratamiento.
- Se base en el consentimiento explícito de la persona interesada.
- Esté autorizada por el derecho de la Unión Europea o de un Estado miembro.

Conviene recordar que, en caso de que se tomen este tipo de decisiones, se informará a la persona interesada.

5.2 Ejercicio de los derechos

5.2.1 ¿Quién puede ejercer estos derechos?

La persona afectada o un representante en su nombre, si se trata de menores de 14 años, personas discapacitadas, personas mayores de 14 años si la ley lo exige, o cuando la persona afectada designe voluntariamente a alguien que la represente.

5.2.2 Procedimiento. ¿Cómo se hacen efectivos los derechos?

- El responsable del tratamiento debe responder a la persona interesada de una forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, especialmente si la información se dirige específicamente a un niño.
- Debe facilitar la respuesta por escrito o por otros medios, incluidos, en su caso, medios electrónicos. Si la persona interesada lo solicita, se le puede dar respuesta verbalmente si demuestra su identidad por otros medios.
- El responsable del tratamiento debe facilitar a la persona interesada el ejercicio de sus derechos y no debe negarse a actuar a petición de la persona interesada salvo cuando pueda demostrar que no está en condiciones de identificar a la persona interesada.
- El responsable del tratamiento debe facilitar a la persona interesada información relativa a sus actuaciones, si la solicitud se ha llevado a cabo de acuerdo con el RGPD y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Este plazo se puede prorrogar dos meses más, en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable debe informar a la persona interesada de cualquiera de estas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando la persona interesada presente la solicitud por medios electrónicos la información se facilitará, siempre que sea posible, por estos mismos medios, salvo cuando la persona interesada solicite que se lleve a cabo de otro modo.
- La información facilitada debe ser gratuita. Si las solicitudes son manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento puede:
    - Cobrar un canon razonable, de acuerdo con los costes administrativos que se han afrontado para facilitar la información o la comunicación, o para llevar a cabo la actuación solicitada.
    - Negarse a actuar respecto a la solicitud.

- El responsable del tratamiento debe soportar la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.
- Cuando el responsable del tratamiento tenga dudas razonables sobre la identidad de la persona física que presenta la solicitud, podrá solicitar la información adicional necesaria para confirmar la identidad de la persona interesada.

5.2.3 ¿Dónde se debe presentar la solicitud?

La persona interesada debe presentar la solicitud ante el responsable del tratamiento, ya sea la escuela que trata sus datos o el Departamento de Enseñanza.

Los derechos pueden ejercerse, además, ante el encargado del tratamiento. En este caso, el encargado (por ejemplo, la empresa que presta el servicio de comedor) debe trasladar la solicitud al responsable para que la resuelva, salvo los casos en que el contrato de encargo del tratamiento lo habilite para resolver las solicitudes por cuenta del responsable.

Si el responsable o, en su caso, encargado del tratamiento, no tramitan la solicitud de la i persona interesada, sin dilación y como máximo al cabo de un mes, se informará a la persona interesada de que se ha recibido su solicitud, de los motivos por los que no se ha atendido y de la posibilidad de presentar una reclamación ante la Autoridad Catalana de Protección de Datos y de ejercer acciones judiciales.

5.2.4 Reclamación ante la falta de atención de los derechos

Las personas interesadas a las que se deniegue en parte o totalmente el ejercicio de los derechos de autodeterminación informativa, o que entiendan que su solicitud se ha desestimado porque no se ha atendido en el plazo establecido, pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos. La APDCAT, a través de la tramitación de un procedimiento de tutela de derechos, resolverá si la denegación es procedente o improcedente

6. El deber de secreto

El responsable del tratamiento y todas las personas que pueden intervenir en cualquiera de las fases del tratamiento de datos de carácter personal están obligados a guardar secreto respecto a estos datos. En este sentido, la LOE establece que el profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor y a la intimidad de los menores o sus familias queda sujeto al deber de sigilo.

Los centros escolares, para el desarrollo de sus funciones, necesitan la colaboración no solo de los profesores, sino también de distintos profesionales: psicólogos, pedagogos, logopedas, maestros de educación especial o educadores sociales. Los centros también cuentan con personal administrativo y otros servicios auxiliares como el de mantenimiento o el comedor. Todos ellos acceden o pueden acceder en algún momento a los sistemas de información o documentación que contienen datos de carácter personal del alumnado.

Para garantizar el cumplimiento de este deber, en una relación jurídica que conlleve el tratamiento de datos de carácter personal, se debe incorporar y definir en los contratos laborales, en los protocolos internos, en las actividades formativas y en las regulaciones específicas que recogen los derechos y obligaciones de las partes. Esta obligación subsiste incluso una vez que cese la relación con el responsable.

El cumplimiento del deber de secreto es aún más importante en un ámbito como el educativo, en el que a menudo se puede tratar información que debe ser especialmente protegida, como la información obtenida por parte de profesionales de las áreas de orientación, psicólogos, pedagogos, logopedas, educación especial y educadores sociales, y que puede incluir diagnósticos, valoraciones y dictámenes profesionales sobre el estado de salud física o psíquica del alumnado o valoraciones sobre su vida personal y familiar.

7. Delegado de protección de datos

7.1 La figura del delegado de protección de datos en las escuelas

Las escuelas están obligadas a designar a un delegado de protección de datos (DPD). Esta obligación se extendería, también, a la escuela concertada y a la escuela privada en el marco del proyecto de la Ley Orgánica de Protección de Datos de Carácter Personal, publicado en el Boletín Oficial de las Cortes Generales núm. 13-1, de 24 de noviembre de 2017.

El delegado de protección de datos podrá formar parte de la plantilla o bien actuar en el marco de un contrato. El delegado de protección de datos de una escuela también lo puede ser de otras escuelas, o bien diferentes escuelas pueden tener un mismo delegado para todas ellas.

Las escuelas deberán publicar los datos de contacto del delegado de protección de datos y comunicar a la Autoridad Catalana de Protección de Datos las designaciones, los nombramientos y los ceses en un plazo de diez días.

El delegado de protección de datos tiene, entre otras, las siguientes funciones:

- Informar y asesorar al centro o al encargado y el personal sobre las obligaciones que impone la normativa de protección de datos.
- Supervisar el cumplimiento de la normativa.
- Asesorar respecto a la evaluación de impacto relativa a la protección de datos.
- Ser el interlocutor del centro escolar con la Autoridad Catalana de Protección de Datos.

La posición del DPD en las organizaciones debe cumplir los requisitos que establece expresamente el RGPD. Entre estos requisitos se encuentran la total autonomía en el ejercicio de sus funciones, la necesidad de que se relacione con el nivel superior de la dirección o la obligación de que el responsable o encargado le faciliten todos los recursos necesarios para desarrollar su actividad.

7.2 ¿Qué requisitos debe cumplir y qué cualificaciones debe tener el delegado de protección de datos?

El DPD se nombrará teniendo en cuenta sus cualificaciones profesionales y, en particular, su conocimiento de la legislación y la práctica de la protección de datos. Esto no significa que el DPD deba tener una titulación específica. Teniendo en cuenta que entre sus funciones se incluye el asesoramiento al responsable o encargado en todo lo referido a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son, sin duda, necesarios; pero también es necesario que cuente con conocimientos ajenos al ámbito estrictamente jurídico, por ejemplo, en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que ejerce su labor.

8. Evaluación de impacto relativa a la protección de datos

Cuando sea probable que un tratamiento suponga un alto riesgo para los derechos y las libertades de las personas, por su naturaleza, alcance, contexto o finalidades, especialmente si se utilizan las nuevas tecnologías, antes de iniciar el tratamiento el responsable tiene que llevar a cabo una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

8.1 ¿Cómo se determina la necesidad de llevar a cabo una evaluación de impacto y qué contenidos debe tener?

El RGPD contiene una lista indicativa de tres supuestos en los que se considera que los tratamientos conllevan un alto riesgo:

- Elaboración de perfiles a partir de los cuales se toman decisiones que producen efectos jurídicos sobre las i personas interesadas o que les afectan significativamente de forma similar.
- Tratamiento a gran escala de categorías especiales de datos.
- Observación sistemática a gran escala de una zona de acceso público.

En las directrices sobre la evaluación de impacto en la protección de datos, EIPD (WP 248), el Grupo del Artículo 29 considera que para valorar si el tratamiento se lleva a cabo a gran escala se debe tener en cuenta lo siguiente:

- El número de personas interesadas 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.

Links

Para la delimitación de la noción de alto riesgo a efectos de la obligatoriedad de llevar a cabo una evaluación de impacto y sobre los criterios para ello, se recomienda consultar la Guía práctica. Evaluación de impacto relativa a la protección de datos de la APDCAT. Guía práctica. Evaluación de impacto relativa a la protección de datos

¿Qué sucede con los tratamientos iniciados antes del 25 de mayo de 2018 a los que, con la nueva normativa, les sea exigible la evaluación de impacto sobre la protección de datos (EIPD)?

Si estos tratamientos se prolongan más allá del 25 de mayo de 2018 y el análisis de riesgo que las organizaciones llevan a cabo sobre los tratamientos iniciados con anterioridad indica que estos tratamientos presentan alto riesgo para los derechos o las liberta des de las personas interesadas, la guía para la evaluación del impacto en la protección de datos también recomienda llevar a cabo una EIPD.

8.2 Consulta previa

En los casos en que las EIPD identifiquen un alto riesgo que, a juicio del responsable del tratamiento, no se pueda mitigar por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable debe consultar a la Autoridad Catalana de Protección de Datos. La consulta debe ir acompañada de la documentación prevista en el RGPD, incluida la propia evaluación de impacto.

Links

Para solicitar una consulta previa, deben seguirse los pasos que se indican en la sede electrónica de la APDCAT: Consulta previa

La Autoridad Catalana de Protección de Datos debe asesorar por escrito al responsable y, en su caso, al encargado, y puede hacer uso de todos los poderes que le confiere el Reglamento, entre los que se incluye el de prohibir la operación de tratamiento.

9. Medidas de seguridad

A diferencia de la normativa actual, el Reglamento no establece una lista de las medidas de seguridad que son de aplicación de acuerdo con la tipología de datos objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas adecuadas al riesgo que conlleva el tratamiento. Esto implica tener que llevar a cabo una evaluación de los riesgos que conlleva cada tratamiento para determinar las medidas de seguridad que deban aplicarse.

9.1 ¿Cómo se lleva a cabo un análisis de riesgos?

Desde el punto de vista de la seguridad de la información, un análisis de riesgos requiere identificar las amenazas (por ejemplo, acceso no autorizado a los datos personales), valorar cuál es la probabilidad de que se produzca una amenaza y el impacto que tendría en las personas afectadas.

El tipo de análisis varía según:

- Los tipos de tratamiento.
- La naturaleza de los datos que se tratan.
- El número de personas interesadas afectadas.
- La cantidad y la variedad de tratamientos que lleva a cabo una misma organización.
- Las tecnologías utilizadas.

Como norma general, en las grandes organizaciones este análisis de riesgos y la determinación de las medidas o controles que se deban implantar se pueden llevar a cabo utilizando alguna de las metodologías o estándares de análisis de riesgo existentes: MAGERIT, ISO, etc. En lo que respecta a responsables de dimensiones menores y con tratamientos de poca complejidad, este análisis puede ser el resultado de una reflexión documentada sobre las implicaciones de los tratamientos en los derechos y las libertades de las personas interesadas. Esta reflexión debe analizar el contexto en que se lleva a cabo el tratamiento (medios, instalaciones, usuarios, etc.) y debe dar respuesta a cuestiones como las siguientes:

- ¿Se tratan categorías especiales de datos?
- ¿Se tratan datos de colectivos vulnerables (por ejemplo, menores)?
- ¿Se tratan datos de un gran número de personas?
- ¿Los datos tratados permiten la elaboración de perfiles?
- ¿La revelación, alteración o pérdida de los datos puede tener consecuencias importantes para las personas afectadas?
- ¿Se tratan los datos fuera de los equipos o las instalaciones del responsable?
- ¿Tienen acceso a los datos terceras personas que prestan servicios por cuenta del responsable?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, (geolocalización, videovigilancia, internet de las cosas, etc.)?

Son muchas las cuestiones que pueden impactar de forma negativa en los derechos y las libertades de las personas si se tratan inadecuadamente sus datos. Por lo tanto, es muy importante que, si no se utiliza una metodología estándar, fácilmente auditable y objetivable, se documenten detalladamente las cuestiones que se han tenido en cuenta a la hora de determinar el nivel de riesgo existente y concretar las medidas de seguridad que deban aplicarse. Esto nos servirá para cumplir con el principio de responsabilidad proactiva.

En cualquier caso, es obvio que cuanto mayor sea el número de respuestas afirmativas, mayor será el riesgo que se puede derivar del tratamiento.

¿Este cambio de enfoque del RGPD conlleva que las medidas que una entidad aplicaba siguiendo el RLOPD no son correctas? No. Quizás son las adecuadas, pero se requiere, en cualquier caso, llevar a cabo el análisis de riesgos para determinar si las medidas aplicadas son correctas o si existe alguna carencia al respecto.

En cualquier caso, las medidas concretas que se apliquen deben garantizar:

- La confidencialidad, la integridad, la disponibilidad y la resiliencia permanentes de los sistemas y de los servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- La existencia de un proceso para verificar y evaluar regularmente la eficacia de las medidas técnicas y organizativas establecidas para garantizar la seguridad del tratamiento.

¿Se pueden seguir aplicando las medidas de seguridad que preveía el RLOPD?

El RGPD no establece ninguna lista de medidas de seguridad basada en los niveles de seguridad básico, medio y alto, como preveía el RLOPD. Deja a criterio del responsable y del encargado, previa evaluación de los riesgos, determinar qué medidas de seguridad se deben aplicar en cada supuesto.

En cualquier caso, se establecerán las medidas de seguridad técnicas y organizativas adecuadas para garantizar un nivel de protección adecuado al riesgo. Las medidas previstas en el RLOPD que ya estén implantadas pueden ser útiles, pero se debe analizar en cada caso si son suficientes o si es necesario modificarlas

9.2 Notificación de violaciones de seguridad de los datos

Violaciones de seguridad de los datos personales: toda 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 forma, o la comunicación o el acceso no autorizados a estos datos.

Situaciones como la pérdida o el robo de un ordenador portátil, el acceso no autorizado a la base de datos (incluso por parte del propio personal), el envío de información personal a un destinatario erróneo, la alteración de datos sin autorización o la pérdida de disponibilidad de los datos (por ejemplo, por haber sufrido un ataque a los sistemas con un software de secuestro, *ransomware*, que cifra los datos) constituyen violaciones de seguridad de los datos y deben ser tratados de acuerdo con lo dispuesto en los artículos 33 y 34 del RGPD.

Si se produce una violación de la seguridad de los datos, el responsable de tratamiento la notificará a la autoridad de control sin dilación indebida y, si es posible, en un plazo máximo de 72 horas, salvo cuando sea improbable que constituya un riesgo para los derechos y las libertades de las personas (artículo 33 del RGPD).

Además, cuando sea probable que la violación comporte un alto riesgo para los derechos de las personas, el responsable deberá comunicarlo a las personas afectadas, sin dilaciones indebidas y en un lenguaje claro y sencillo, a menos que:

- El responsable haya adoptado medidas de protección adecuadas, tales como que los datos no sean inteligibles para personas no autorizadas.
- El responsable haya aplicado medidas posteriores que garanticen que ya no existe la probabilidad de que se concrete el alto riesgo.
- Suponga un esfuerzo desproporcionado (artículo 34 del RGPD).).9.2.1 ¿Cuál es el plazo para notificar una violación de seguridad de los datos a la autoridad de control?

La notificación de la violación de seguridad a las autoridades debe producirse sin dilación indebida y, si es posible, dentro de las 72 horas siguientes al momento en que el responsable haya tenido constancia de ella. Este criterio puede ser objeto de distintas interpretaciones. En general, se considera que se tiene constancia de una violación de seguridad cuando existe una certeza razonable de que se ha producido un incidente de seguridad que ha comprometido los datos personales y se tiene un conocimiento suficiente de la naturaleza y el alcance de este incidente. La mera sospecha de que ha habido una violación, sin que se conozcan mínimamente sus circunstancias, todavía no debería 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.

Sin embargo, en casos de violaciones que, por sus características, puedan tener un gran impacto, sí puede ser recomendable contactar con la autoridad de supervisión tan pronto como haya evidencias de que se ha producido una situación irregular respecto a la seguridad de los datos. Lo anterior, sin perjuicio de que estos primeros contactos se completen con una notificación formal, más completa, dentro del plazo legalmente previsto.

Si la notificación a la autoridad de control no se produce en el plazo de 72 horas, deberá ir acompañada de una explicación de los motivos que han ocasionado el retraso.

9.2.2 ¿Cuál debe ser el contenido de la notificación de una violación de la seguridad de los datos a la autoridad de control?

La notificación debe contener unos elementos mínimos que el propio RGPD establece (artículo 33 del RGPD) y que incluye la naturaleza de la violación, las categorías y el número aproximado de datos afectados, las medidas adoptadas por el responsable para solucionar la violación y, en su caso, las medidas aplicadas para paliar los posibles efectos negativos sobre las personas afectadas.

Si no es posible facilitar simultáneamente toda la información, se puede facilitar de forma gradual, sin dilación indebida.

Links

Para comunicar una violación de seguridad deben seguirse los pasos que se indican en la sede electrónica o en el sitio web de la APDCAT:

- En la sede de la APDCAT
- En la web de la APDCAT

Con independencia de la notificación a las autoridades, los responsables deben documentar todas las violaciones de seguridad. Se trata de una obligación que establece el RGPD y que se aproxima mucho al registro de incidencias que preveía el RLOPD.

9.2.3 ¿Cuándo es probable que una violación de seguridad comporte un riesgo alto para los derechos de las personas afectadas?

El criterio del alto riesgo que menciona el RGPD debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños importantes a las personas

interesadas. Esto puede suceder, por ejemplo, si se revela información confidencial, como contraseñas o la participación en determinadas actividades, si se difunden datos sensibles o si se pueden producir perjuicios económicos para las personas afectadas.

9.2.4 ¿Cuál es la finalidad de comunicar una violación de seguridad a las personas afectadas?

El objetivo de esta comunicación debe ser permitir que las personas afectadas puedan tomar medidas para protegerse de las consecuencias de la violación de seguridad. Por ello, el RGPD requiere que se les comunique sin dilación indebida y sin hacer referencia ni al momento en que se tiene constancia de ella ni a la posibilidad de efectuar la comunicación dentro de un plazo de 72 horas. El propósito es siempre que la persona interesada afectado pueda reaccionar tan pronto como sea posible.

Por los mismos motivos, el RGPD añade a los contenidos de la notificación que, en caso de que sea necesario, deberán establecerse recomendaciones sobre las medidas que pueden tomar las personas afectadas para hacer frente a las consecuencias de la violación.

9.2.5 ¿Qué puede suceder si no se notifica una violación de seguridad de los datos?

Si una violación de seguridad no se notifica a la autoridad de control, se puede incurrir en la vulneración de una obligación prevista en el RGPD, salvo cuando sea improbable que la violación suponga un riesgo para los derechos y las libertades de las personas físicas.

También puede constituir una vulneración del RGPD el hecho de notificar la violación de seguridad de datos más allá de las 72 horas, si no existen razones que lo justifiquen. Estas vulneraciones pueden conllevar que se ejerzan poderes de investigación y correctivos, incluida la imposición de una multa, en su caso.

Por el contrario, no hay ninguna penalización si se notifica a la autoridad un incidente de seguridad que no llega a tener la consideración de violación de seguridad de datos personales de notificación obligada.