Protección de datos desde la óptica de las personas responsables y encargadas de tratamiento. Curso avanzado

Jorge Viguri Cordero

23 de octubre de 2023

UNIVERSITAT JAUME I

#ProDigital

ÍNDEX

01. Contexto normativo y ámbito de aplicación

1. Régimen jurídico aplicable

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (Reglamento general de protección de datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establecen el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales. Con esta normativa vigente, se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo previsto en la disposición adicional decimocuarta de la LOPDGDD, y siguen vigentes las disposiciones de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que no contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y la LOPDGDD.

Por lo que concierne a la LOPDGDD, tiene como objetivo el adaptar el ordenamiento español al RGPD, aplicable desde el 25 de mayo de 2018. Por su parte, incorpora la novedad de la garantía de los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución española (CE). Esto es debido a que, cada vez más, los medios que se utilizan para el tratamiento de datos personales son y serán digitales. Por eso, cada día más, cobra especial importancia la ciberseguridad en las organizaciones, dado que es la principal fuente de amenazas. No establece novedades con respecto a lo establecido en el RGPD, excepto en la edad legal para poder prestar el consentimiento explícito, que se fija en los 14 años. En cuanto al ámbito laboral se establecen temas clave como el derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo, el respeto del tiempo de descanso del trabajador, permisos y vacaciones, así como de su intimidad personal y familiar. Se trata con ello de potenciar el derecho a la conciliación de la actividad laboral y la vida personal y familiar. Asimismo, con esta ley se quiere garantizar

el derecho a la intimidad del trabajador, en materia de grabación de videovigilancia, tanto de imagen como de sonido, evitándose la grabación de imágenes y sonido en las zonas de descanso y la grabación de sonido se restringe a centros de trabajo en caso de riesgos relevantes para la seguridad de las instalaciones, bienes y personas y respetando siempre el principio de proporcionalidad e intervención mínima.

Artículo 1. Objeto de la ley

La presente ley orgánica tiene por objeto: a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. 2. Esta ley orgánica no será de aplicación: A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo. a) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3. b) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y

supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

Artículo 3. Datos de las personas fallecidas

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

4. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Definiciones

- **DATOS PERSONALES**: toda información sobre una persona física identificada o identificable («el 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. Los datos relativos a una persona jurídica, como el domicilio, la denominación social o el CIF, no tienen la consideración de datos de carácter personal, por ende, no resultará de aplicación el RGPD.
- **TRATAMIENTO:** cualquier operación llevada a cabo sobre datos personales o conjuntos de datos personales, ya sea por procedimientos 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.
- **SEUDONIMIZACIÓN:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. ⟩ FICHERO: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

- **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:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **DESTINATARIO:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, NO se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros.
- **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.
- **CONSENTIMIENTO DEL INTERESADO:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- **REPRESENTANTE**: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del RGPD.
- **EMPRESA:** persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

3. Algunas notas de interés en la figura de responsable y encargado del tratamiento

- ¿Qué es un encargado del tratamiento y cuál es su función principal?

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste. Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales. Así, podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales (por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores) y otros que tratan datos personales sólo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento (por ejemplo el gestor de un servicio público municipal). Pese a que la definición puede parecer clara, en la práctica se dan multitud de situaciones donde puede ser difícil deslindar cuándo estamos frente a un encargado o a un responsable del tratamiento.

Para facilitar esta distinción, debemos tener en cuenta que corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones de quien le encomienda un determinado servicio, respecto al correcto tratamiento de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio. Cuando sea de aplicación el texto Refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, debe tenerse en cuenta que dicha ley prevé (disposición adicional 26ª) que, cuando la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, el contratista tendrá la consideración de encargado del tratamiento. En estos casos también será de aplicación el régimen establecido en el RGPD.

¿Qué tratamientos puede llevar a cabo un encargado sobre los datos que le han sido encomendados?

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: 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. En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte

¿Qué nivel de decisión puede asumir un encargado del tratamiento?

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades. Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por el responsable del tratamiento

¿Puede el responsable del tratamiento elegir cualquier encargado del tratamiento?

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 tanto, un deber de diligencia en la elección del responsable. El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento. Para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o la posesión de un certificado de protección de datos pueden servir como mecanismos de prueba.

¿Cómo deben regularse las relaciones entre el responsable y el encargado del tratamiento?

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico. La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento. En cualquier caso, ya se trate de un acuerdo o de otro acto jurídico, su contenido debe reunir los requisitos establecidos en el RGPD, a los que más adelante se hace referencia. El contenido del acto o acuerdo puede basarse en cláusulas tipo establecidas por la Comisión Europea o por la autoridad de control, inclusive cuando formen parte de una certificación otorgada al responsable o al encargado del tratamiento. Los modelos de cláusulas que se incluyen en el Anexo 1 de este documento no tienen la consideración de cláusulas tipo a los efectos del artículo 28.8 del RGPD, sino que son simplemente un modelo orientativo para que los diferentes responsables puedan adaptarlo a las necesidades derivadas de su propia organización.

El contenido mínimo de un acuerdo o acto de encargo del tratamiento que incluya el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

¿Quién es responsable de los tratamientos realizados por el encargado?

El responsable del tratamiento no pierde esta consideración en ningún caso y, por tanto, continúa siendo responsable del correcto tratamiento de los datos personales y de la garantía de los derechos de las personas afectadas. El responsable tiene una obligación de especial diligencia en la elección y supervisión del encargado.

¿El RGPD se aplica sólo a los encargados establecidos en el territorio de la Unión Europea?

No, el Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Por otra parte, el RGPD también se aplicará al tratamiento de datos personales de interesados que residan en la Unión realizado por un encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se les requiere su pago.

b) El control de su comportamiento, en la medida en que tenga lugar en la Unión.

02. Principios y legitimación del RGPD y LOPDDGDD

1. Principios de protección de datos

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales:

- **Principio de "licitud, transparencia y lealtad",** que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- **Principio de "finalidad"** que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- **Principio de "minimización de datos**", es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento

reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.

- **Principio de "exactitud",** que obliga a los responsables a disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- **Principio de "limitación del plazo de conservación"** que constituye una de las materializaciones del principio de minimización. La conservación de esos datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.
- **Principio de "seguridad"** que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.
- **Principio de "responsabilidad activa"** que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

2. Las bases legitimadoras de los tratamientos

Para que un tratamiento de datos personales sea lícito debe **contar con una base legitimadora** con el fin de ampararse en alguna de las seis bases habilitantes establecidas con carácter tasado en el artículo 6.1 RGPD, cuyo tenor es el siguiente:

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

*a) el interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;*

*b) el tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*

*c) el tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento;*

*d) el tratamiento es necesario para **proteger intereses vitales** del interesado o de otra persona física;*

*e) el tratamiento es necesario para el **cumplimiento de una misión realizada en interés público** o **en el ejercicio de poderes públicos** conferidos al responsable del tratamiento;*

*f) el tratamiento es necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

⇒ En consecuencia, antes de comenzar a tratar datos personales, **debe identificarse la base legitimadora**. En caso de carecer de ella, el tratamiento es ilícito con independencia de que observen las demás exigencias normativas.

3. ¿Se pueden recabar y tratar datos personales de menores?

Sí, siempre que se observe lo dispuesto en el RGPD. Cuando la recogida y tratamiento de datos de menores responda al consentimiento, hay que tener en cuenta que deberá ser expreso y que cuando se trate de menores de 14 años lo han de prestar sus padres o tutores.

Los mayores de esa edad pueden prestar ellos mismos el consentimiento para que se recojan sus datos, salvo en aquellos casos en los que la Ley exigiera que estén asistidos por su padres o tutores.

El Código Civil estipula que la patria potestad se ejercerá por ambos progenitores o por uno de ellos con el consentimiento expreso o tácito del otro, siendo válidos los actos que realice uno de ellos conforme al uso social y a las circunstancias o las situaciones de urgente necesidad. En caso de desacuerdo, cualquiera de los dos podrá acudir al Juez, quién decidirá al respecto.

En el supuesto de padres separados en el que la guarda y custodia del hijo menor ha sido atribuida a uno de los progenitores, pero ambos conservan la patria potestad, de no alcanzarse un acuerdo habrá de someterse la cuestión al Juez correspondiente.

Véase Canal menores de la AEPD

4. ¿Puede un menor de 14 años ejercitar los derechos contemplados en el RGPD?

Además del derecho de información, el RGPD permite que los afectados puedan ejercitar los derechos de acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento, y derecho de oposición a las decisiones automatizadas (incluyendo la elaboración de perfiles).

Estos derechos se ejercitarán ante el responsable del tratamiento. También es posible ejercitarlos en los casos de que existiese un encargado de tratamiento ante éste, siempre y cuando el responsable y dicho encargado así lo hubiesen convenido.

En el caso de los menores de 14 años el ejercicio de estos derechos se realizará siempre por **quien ostente la patria potestad o por sus tutores**. Los mayores de 14 años se encuentran habilitados para el ejercicio de los derechos.

5. Plazos de conservación de los datos

La AEPD ha determinado que corresponde al propio DPD asesorar al responsable del tratamiento y establecer los plazos de conservación de los datos que trata la empresa a través de un examen pormenorizado de todos y cada uno de los tratamientos contenidos en el Registro de Actividades de Tratamiento conforme a la legislación vigente, aunque no era competente para pronunciarse sobre los plazos de prescripción de una entidad en específico.

Sin embargo, proporciona una delimitación general de los plazos de conservación de los datos en distintos ámbitos, respecto de los datos suprimidos:

- Obligaciones personales (art. 1964.2 CC): Bloqueo durante 5 años.
- Libros y documentos del empresario (art. 30 CCom): Bloqueo durante 6 años.
- Tributos (LGT y CP): 4 años para la prescripción de deudas tributarias, aunque en ocasiones se deba conservar durante 10 años.
- Seguridad Social (art. 21 LISOS y 131 CP): Conservación hasta 10 años.
- Ámbito Laboral (art. 59 TRLET): Bloqueo durante 1 año.
- Prevención de Riesgos (art. 22 LPRL): Puede llegar hasta los 40 años, dependiendo del sector y del desarrollo normativo de aplicación.
- Responsabilidad relacionada con el propio tratamiento de datos personales: bloqueo durante 3 años.
- Derecho a indemnización y responsabilidad del RGPD: bloqueo hasta 1 año.

Así, en cuanto al plazo de conservación previsto en el artículo 5.1.e) RGPD y de la obligación de “bloqueo” prevista en el artículo 32 de la LOPDGDD, la AEPD entiende que el bloqueo excluye el borrado material de los datos, siempre y cuando ello sea de conformidad con las limitaciones previstas en el propio artículo 32.

Estas limitaciones excluyen el borrado material de los datos personales solo en las siguientes circunstancias: 1. para la puesta a disposición de los datos a los jueces y

tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, y 2. para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de estas. Este último punto debe interpretarse como el "plazo de prescripción de las acciones" encaminadas a la exigencia de tales responsabilidades.

03. Adecuación a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

1. Transparencia y protección de datos

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, establece que todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley.

La información pública se define como los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder alguno de los sujetos incluidos en el ámbito de aplicación del Título I de esta Ley, y que hayan sido elaborados o adquiridos en el ejercicio de sus competencias.

Si la información solicitada contiene datos de carácter personal ¿Prevalece el derecho a la protección datos o debe entregarse la información?

En este caso, y atendiendo al artículo 15 de la Ley 19/2013, de 9 de diciembre, deberá tenerse en cuenta lo siguiente:

- Si los datos son sensibles (relativos a ideología, afiliación sindical, religión o creencias), el acceso únicamente se podrá autorizar en caso de que se obtenga el

consentimiento expreso y por escrito del afectado, salvo que éste hubiese hecho manifiestamente públicos los datos con anterioridad.

- Si los datos son sensibles (reveladores de origen racial, salud y a la vida sexual origen racial, a la salud o a la vida sexual, genéticos o biométricos) o relativos a la comisión de infracciones penales o administrativas que no supongan amonestación pública al infractor, será necesario para conceder el acceso el consentimiento expreso del afectado o que exista una norma con rango Legal que habilite el acceso.
- Si los datos son meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, con carácter general, y salvo que prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos, se concederá el derecho de acceso.

Si los datos no tuviesen la condición de especialmente protegidos, debe realizarse una ponderación del interés público en la divulgación de la información y los derechos de los afectados. Esta ponderación se realizará de conformidad con los siguientes criterios:

A) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.
B) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

No será de aplicación los puntos anteriores si la información se facilita de forma disociada, es decir, que impida la identificación de las personas afectadas.

Algunos aspectos prácticos relevantes:

Sobre el "posible" acceso a la documentación del resto de candidatos de un concurso-oposición

Si el solicitante ostenta la condición de interesado:

En el caso de los procedimientos de concurrencia competitiva, la AEPD ha considerado que **debe poder accederse a los datos alegados** para obtener una plaza por aquéllos con quien se compita. No obstante, cabe limitar el acceso o la entrega de copias de la documentación obrante en el expediente, por razones de eficacia administrativa o a efectos de proteger la intimidad de los restantes interesados, a los datos y copias relevantes para la tutela de los derechos e intereses de quienes las solicitan.

Asimismo, no podrán utilizar los datos a que tengan acceso para una finalidad distinta a aquélla de la defensa de su derecho en el procedimiento de que se trate o posteriormente en vía judicial. De este modo la utilización para otras finalidades, su comunicación a terceros o su divulgación pueden ser constitutivas de una infracción a lo previsto en la LOPD.

Si el solicitante no ostenta la condición de interesado:

Para determinar el acceso debe aplicarse lo dispuesto en la Ley de Transparencia, Acceso a la Información y Buen Gobierno. De esta forma, el acceso a los documentos aportados por el candidato seleccionado a los datos especialmente protegidos se realizará de conformidad a la aplicación del apartado 1 del artículo 15 de la Ley 19/2013.

Respecto de los restantes datos, el órgano al que se solicitan deberá realizar una ponderación razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la misma, resultando, a juicio de esta Agencia, de interés aquí los criterios contenidos en las letras b) y d) del apartado 3 del mencionado artículo 15.

Sobre la “posibilidad” de publicar las actas de un órgano colegiado incluyendo las deliberaciones de cada uno de sus miembros

El artículo 7 de la Ley de Transparencia no prevé la publicación de las actas de los órganos colegiados, sino únicamente de la información jurídica que enumera el precepto. Además, de lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, no se desprende que el acta haya de incorporar todas y cada una de las manifestaciones efectuadas por los miembros del órgano colegiado.

La referencia a los puntos principales de las deliberaciones en ningún caso parece exigir la indicación de la manifestación de cada uno de los integrantes del órgano. Antes bien, el artículo 19.5 prevé que esta información, cuando sea discrepante, se incluirá en el acta a instancias del propio miembro del órgano, dado que se indica que "en el acta figurará, a solicitud de los respectivos miembros del órgano, el voto contrario al acuerdo adoptado, su abstención y los motivos que la justifiquen o el sentido de su voto favorable.

Asimismo, cualquier miembro tiene derecho a solicitar la transcripción íntegra de su intervención o propuesta, siempre que aporte en el acto, o en el plazo que señale el Presidente, el texto que se corresponda fielmente con su intervención, haciéndose así constar en el acta o uniéndose copia a la misma". Igualmente, conforme al artículo 19.5 "los miembros que discrepen del acuerdo mayoritario podrán formular voto particular por escrito en el plazo de dos días, que se incorporará al texto aprobado".

Por lo tanto, por una parte, la Ley 19/2013 no impone la publicación íntegra de las actas y que, por otra, la Ley 40/2015 no exige que las mismas incorporen expresamente las distintas manifestaciones efectuadas durante las deliberaciones de los órganos colegiados por sus miembros.

2. Registro de actividades de tratamiento

Una de las herramientas que el RGPD exige a los responsables para demostrar la conformidad con el RGPD es el mantenimiento de los registros de actividades de

tratamientos de datos que tienen bajo su responsabilidad y control, teniendo en cuenta la obligada colaboración con la Autoridad de Control que exige poner a su disposición dichos registros de operaciones de tratamiento para facilitar las actividades de supervisión realizadas en el ámbito de los poderes que el RGPD le otorga.

El RGPD y la LOPDGDD exigen un contenido mínimo que deberá ser tenido en cuenta por el responsable:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

El contenido del Registro de Actividades de Tratamiento constituye una información mínima exigible. Este registro podría integrarse y formar parte de los catálogos de procesos que ya existiesen en la entidad, incluyendo toda la información que el responsable considere necesaria para proteger los derechos y libertades de las personas físicas y poder demostrar cumplimiento atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento,

así como los posibles orígenes de los riesgos que dicho tratamiento pudiera suponer para los interesados. El registro podría incluir aspectos que faciliten la aplicación efectiva de la responsabilidad proactiva como: análisis de riesgos para los derechos y libertades realizados, la descripción sistemática del tratamiento, los sistemas de información sobre los que se apoya, la descripción de la identidad de los encargados del tratamiento, las garantías previstas para llevar a cabo transferencias internacionales de datos, información de contacto de las personas o los departamentos de la organización que se encuentran implicados en las operaciones de tratamiento, etc.

En el caso de dar acceso al contenido del Registro de Actividades de Tratamiento, y con relación a una posible descripción general de las medidas técnicas y organizativas de seguridad, debe evitarse desvelar cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad. En este caso, se recomienda contar con el Responsable de Seguridad o CISO con carácter previo a la publicación de dicha descripción general o, en su caso, utilizar una referencia general a los estándares de seguridad utilizados.

3. Facilita RGPD

La mera obtención de los documentos que proporcionan las herramientas de la AEPD no supone, en ningún caso, el cumplimiento automático de las obligaciones que el RGPD y la LOPDGDD establecen para los responsables y encargados de los tratamientos de datos personales, en particular lo referido al principio de responsabilidad activa que el RGPD desarrolla en su Capítulo IV. Se trata de documentos iniciales de ayuda orientados a facilitar la comprensión de dichas obligaciones y abordarlas, inicialmente, de forma adecuada.

Sobre la base de los documentos obtenidos los responsables y encargados de los tratamientos de datos personales deberán llevar a cabo cuantas adaptaciones fueran necesarias de forma particularizada para cada tratamiento de datos personales; teniendo en cuenta los riesgos que para los derechos y libertades de las personas físicas pudieran

derivar de dichos tratamientos en función de su naturaleza, su alcance, su contexto y sus finalidades (Considerando 76 y Artículo 35.1 del RGPD).

El Reglamento General de Protección de Datos (RGPD) se aplica desde el 25 de mayo de 2018. Con la finalidad de facilitar la adecuación al RGPD a las empresas y profesionales (personas responsables o encargadas de tratamientos) que traten datos personales de escaso riesgo para los derechos y libertades de las personas, la Agencia Española de Protección de Datos pone a su disposición la herramienta.

Facilita RGPD es una herramienta fácil y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia en ningún caso puede conocer la información que haya sido aportada.

Ha sido diseñada como un recurso útil para cualquier empresa o profesional, ya que con tan solo tres pantallas de preguntas muy concretas permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si se adapta a los requisitos exigidos para utilizar Facilita RGPD o si debe realizar un análisis de riesgos.

Facilita RGPD no podrá utilizarse para tratamientos que impliquen un alto riesgo para los derechos y libertades de las personas, como datos de salud o tratamientos masivos de datos, entre otros.

La herramienta genera diversos documentos adaptados a la empresa concreta, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargado de tratamiento, el registro de actividades de tratamiento, y un anexo con medidas de seguridad orientativas consideradas mínimas.

Facilita RGPD está orientada a empresas que tratan datos personales de escaso riesgo, como por ejemplo, datos personales de clientes, proveedores o recursos humanos.

Tenga en cuenta que Facilita RGPD es una ayuda y, por tanto, la documentación resultante deberá estar adaptada y actualizada a la situación de los tratamientos que se lleven a cabo en su entidad. La obtención de los documentos no implica el cumplimiento automático del RGPD.

Acceso a **FACILITA 2.0:** https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQ4NjI3NzAxNjk4MDU1NjcxMzY4?updated=true

4. Realización de evaluaciones de impacto de protección de datos

El RGPD introduce el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD) y obliga a las Autoridades de Control a establecer listas orientativas de tratamientos que no requieren EIPD, así como de tratamientos que sí requieren su realización. Puede consultar las listas orientativas de tratamientos que no requieren EIPD publicadas por la AEPD y aprobadas por el EDPB aquí:

Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)

Puede consultar la lista orientativa de tratamientos que requieren EIPD publicada por la AEPD y aprobada por el EDPB aquí:

Listas de tipos de tratamientos de datos que requieren Evaluación de impacto relativa a protección de datos (art 35.4)

Con carácter general, existe la obligación de llevar a cabo la realización de una EIPD siempre que el tratamiento implique un alto riesgo para los derechos y libertades de las personas físicas. No obstante, con independencia de esta obligación, el responsable podrá llevar a cabo la EIPD cuando lo considere o valore necesario, **estas listas son orientativas y no restrictivas**.

Puede consultar los recursos de ayuda publicados por la AEPD para realizar la evaluación del riesgo y la EIPD en el área de actuación de innovación y tecnología de nuestra web.

I. Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
II. **Relación de tablas de la guía de Gestión del riesgo y evaluación de impacto en formato editable**
III. **Lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa**
IV. Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)
V. Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)
VI. Instrucción 1/2021 de la AEPD de directrices respecto de la función consultiva de la Agencia. Capitulo IV: Consultas Previas
VII. Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas
VIII. **Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado**
IX. EDPS: Guía para evaluar la proporcionalidad de los tratamientos en políticas y medidas legislativas
X. EDPS: Guía para evaluar la necesidad de los tratamientos en políticas y medidas legislativas
XI. Herramienta EVALUA-RIESGO para el análisis de los factores de riesgo
XII. **Herramienta de ayuda para empresas que realicen un tratamiento de datos personales de escaso riesgo para el cumplimiento del RGPD: FACILITA-RGPD**
XIII. **Herramienta para ayudar a las personas emprendedoras y startups tecnológicas a cumplir con la normativa de protección de datos: FACILITA-EMPRENDE**
XIV. Herramienta básica para la realización de análisis de riesgos y evaluaciones de impacto en protección de datos

5. Notificación de brechas de datos personales a la Autoridad de Control

Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

Con el objetivo de ayudar en la toma de decisiones, la AEPD ofrece la herramienta ASESORA BRECHA.

El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además cuando el riesgo sea alto el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD.

El plazo para notificar a la autoridad de control es de 72 horas desde que la organización tiene constancia de la brecha.

En el ámbito privado, los responsables del tratamiento afectados por una brecha de datos personales deberán notificar a la AEPD:

- Cuando su único establecimiento esté localizado en España.

- Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
- Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

En el ámbito público, con carácter general las AAPP deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción del caso de las Comunidades Autónomas de:

- Andalucía
- Cataluña
- País Vasco

Cuando las brechas de datos personales se produzcan en entidades del sector público bajo su competencia.

Las notificaciones de brechas de datos personales a la AEPD se deben realizar de forma electrónica, usando el formulario de notificación de brechas de datos personales de la Sede Electrónica para garantizar una correcta ejecución de las obligaciones del artículo 33.3 del RGPD.

La notificación a la autoridad de control de una brecha que afecta a datos personales forma parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla no implica necesariamente la apertura de un procedimiento administrativo. De hecho, notificar en tiempo y forma es una evidencia de la diligencia de la organización, mientas que no cumplir con esa obligación si está tipificado como infracción.

Sin embargo, en aquellos casos en los que el responsable considere que no existieran riesgos para los derechos y libertades de las personas físicas el responsable tiene la

obligación de documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el artículo 33 del RGPD.

Con el objetivo de ayudar en la obligación de notificar las brechas de datos personales a la autoridad de control, la AEPD ofrece indicaciones en la Guía para la notificación de brechas de datos personales así como otros recursos en el apartado de **innovación y tecnología**

04. Delegado de protección de datos y gestión de riesgos

1. El Delegado de Protección de Datos

DESIGNACIÓN:

a) Por los responsables y encargados obligatoriamente en los supuestos previstos en art. 37.1 del RGPD, y voluntariamente en el resto de los casos.
b) Su nombramiento será comunicado a la Agencia Española de Protección de Datos y a la Autoridad Autonómica.

CUALIFICACIÓN -> Tendrá titulación Universitaria que acredite conocimientos especializados en materia de datos.

POSICIÓN:

1. Actuará de interlocutor del responsable ante la Agencia Española y las autoridades autonómicas.
2. No podrá ser removido ni sancionado en el ejercicio de sus funciones por el responsable, salvo dolo o negligencia.
3. Se garantizará su independencia dentro de la organización.
4. Si apreciase alguna vulneración lo comunicará al órgano de administración y al responsable o encargado.

INTERVENCIÓN DEL DELEGADO EN RECLAMACIONES:

a) En caso de reclamación, el interesado, previamente a la reclamación a la Agencia Española, podrá dirigirse al Delegado de la entidad. En este caso responderá a la reclamación en un plazo de 2 meses a contar desde la entrada de la reclamación.
b) Si la reclamación se hace directamente a la Agencia Española, entonces dispondrá de un plazo de 1 mes para responder. Si transcurrido el plazo no hay contestación, se estará a lo dispuesto en el Título VIII de esta Ley.

Es importante destacar que, en caso de que se externalicen las funciones del DPD a un tercero, éste tiene la consideración de encargado del tratamiento por cuando el DPD debe poder acceder a los datos que se traten. Por tanto, deberá formalizarse un encargo del tratamiento.

2. La Agencia Española de Protección de Datos

DEFINICIÓN:

- Es la Autoridad Administrativa independiente con personalidad jurídica y plena capacidad pública y privada en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del Ministerio de Justicia.
- Actuará de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.
- Comunidades autónomas que tienen designada una autoridad de control: Cataluña, País Vasco y Andalucía.
    - Consejo de Transparencia y Protección de Datos
    - Autoridad Catalana de Protección de Datos
    - Agencia Vasca de Protección de Datos

REGIMEN JURÍDICO:

- Se rige por lo dispuesto en el RGPD, la presente ley orgánica y sus disposiciones de desarrollo. Supletoriamente la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (RJSP).
- El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto.

FUNCIONES MÁS DESTACADAS -> general: velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Específicas:

• controlar la aplicación del RGPD y el resto de la normativa de protección de datos, así como proceder a que se aplique.

• Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a personas menores de edad deberán ser objeto de especial atención.

• Promover la sensibilización de las personas responsables y encargadas del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento.

• Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros.

• Tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80 del RGPD, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran

necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control.

• Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento.

• Llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública.

• Hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.

• Adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d) del RGPD.

• Elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4 del RGPD.

• Ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2 del RGPD.

• Alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5 del RGPD.

• Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5 del RGPD.

- Llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7 del RGPD.

- Elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del RGPD.

- Efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del RGPD.

- Autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3 del RGPD.

- Aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47 del RGPD.

- Contribuir a las actividades del Comité.

- Llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2 del RGPD.

- Desempeñar cualquier otra función relacionada con la protección de los datos personales.

Otros poderes: de investigación y correctivos

De investigación.

- Ordenar a la persona responsable y al encargado del tratamiento y, en su caso, al representante de la persona responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones.
- Llevar a cabo investigaciones en forma de auditorías de protección de datos.

- Notificar a la persona responsable o al encargado del tratamiento las presuntas infracciones de la normativa de protección de datos.
- Obtener de la persona responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones.
- Obtener el acceso a todos los locales de la persona responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

Correctivos.

- Sancionar a toda persona responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en la normativa de protección de datos.
- Sancionar a toda persona responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en la normativa de protección de datos.
- Ordenar a la persona responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente RGPD.
- Ordenar a la persona responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones de la normativa de protección de datos, cuando proceda, de una determinada manera y dentro de un plazo especificado.
- Ordenar a la persona responsable del tratamiento que comunique a la persona interesada las brechas de seguridad de los datos personales.
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19 del RPGD.

- Retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43 del RGPD, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación.
- Imponer una multa administrativa con arreglo al artículo 83 del RGPD, además o en lugar de las medidas mencionadas en el presente apartado, 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.

3. Procedimientos en caso de vulneración de la protección de datos

RÉGIMEN JURÍDICO: procedimientos tramitados por la Agencia Española en los supuestos: a) El afectado reclame que su solicitud no ha sido atendida en el ejercicio de sus derechos. b) Investigaciones sobre infracciones al Reglamento y Ley Orgánica.

FORMA DE INICIACIÓN: a) Si es por falta de atención en la solicitud (a) -> se procederá a la admisión a trámite, y una vez aprobado, tendrá 6 meses para resolver. Transcurrido el plazo, el interesado la podrá considerar estimada. b) Si es por la existencia de infracción (b) -> podrán darse dos supuestos:

a) PROPIA INICIATIVA -> se iniciará mediante Acuerdo de Inicio.
b) RECLAMACIÓN -> que precederá de ser Admitida a trámite. El procedimiento tendrá una duración de 9 meses, transcurridos los cuales, si no hay resolución, se entenderá su caducidad y en consecuencia archivo de actuaciones.

ADMISIÓN A TRÁMITE DE LAS RECLAMACIONES: podrán no ser admitidas cuando: a) No versen sobre protección de datos. b) Sin fundamento. c) Sean abusivas. d) No se observe infracción. e) Si la empresa ha adoptado medidas correctoras, siempre que: 1. No haya causado perjuicio al afectado. 2. Sus derechos no se vean afectados Plazo para notificar al

interesado la admisión: 3 meses, una vez transcurrido dicho plazo, se entenderá por admitida.

ACTUACIONES PREVIAS DE INVESTIGACIÓN: 1. Se realizarán antes de adoptar el acuerdo de inicio y una vez admitida a trámite. 2. No podrán tener una duración superior a 12 meses desde la fecha del acuerdo de admisión.

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR: concluidas las actuaciones previas, la Presidencia dictará acuerdo de inicio donde se concretará: 1. Los hechos. 2. Identificación de las personas. 3. Infracciones cometidas y posibles sanciones.

MEDIDAS PROVISIONALES: la Agencia Española podrá dictaminar las medidas provisionales NECESARIAS y PROPORCIONALES. Podrán consistir en: 1. Bloqueo de datos y cesación de su tratamiento. 2. En caso de incumplimiento, podrá proceder a la inmovilización.

UNIVERSITAT JAUME I

#ProDigital