Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Guía de transición para la LOPD: los nuevos derechos.

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Carlos Giménez Hervás

Tutor: Juan Vicente Oltra Gutiérrez

Curso 2018/2019

Resumen

La necesidad de adaptación de España al Reglamento General de Protección de Datos causó el desarrollo de una nueva ley de protección de datos, llamada Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, que se adecuase al reglamento europeo y que garantizase la protección de las personas físicas, en lo que respecta al tratamiento de sus datos personales. Este trabajo proporciona todos los datos necesarios para ser capaz de cumplir la normativa de protección de datos tras los cambios provocados por la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Adicionalmente se describe el proceso llevado a cabo para la creación de una lista de tareas pendientes mediante el software de hojas de cálculo llamado "Microsoft Excel", que pueda ser de utilidad para los encargados de protección de datos.

Palabras clave: guía, protección, datos, LOPD, delegado, DPD, encargado, responsable, derechos, AEPD, normativa.

Abstract

The need to adapt Spain to the General Data Protection Regulation caused the development of a new data-protection law, called Organic Law on the Protection of Personal Data and the Guarantee of Digital Rights, that fits to the European regulation and guarantees the protection of physical persons, with regard to the processing of their personal data. This work provides all necesary information to be able to follow the data-protection rules after the changes caused by the entry into force of the Spanish Organic Law 3/2018, of 5 december, on the Protection of Personal Data and the Guarantee of Digital Rights. Additionally, it describes the process carried out to create a to-do list using the spreadsheet software called "Microsoft Excel", which may be useful to processors.

Keywords : guide, protection, data, LOPD, delegate, DPO, processor, controller, rights, AEPD, rules.

Tabla de contenidos

1. Introducción

El 13 de diciembre de 1999 se aprobó en España la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Dicha ley carecía de muchos aspectos que han adquirido importancia a lo largo de los años, sobre todo los relacionados con los medios digitales.

El 27 de abril de 2016, en Bruselas, se creó el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de la Unión Europea, que sería aplicable a partir del 25 de mayo de 2018 por todos los estados miembros de la Unión Europea, esto obligó a España a crear rápidamente el 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, que entró en vigor el 31 de Julio de 2018.

El 7 de diciembre de 2018, con la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, se deroga el Real Decreto de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos y la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Además, la LOPDGDD genera modificaciones en otras normas indicadas en las disposiciones finales de la misma.

La entrada en vigor de la LOPDGDD generó una necesidad de conocimiento sobre los cambios respecto a la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 en todas las empresas.

1.1 Objetivos

El principal objetivo de este trabajo es generar la información necesaria sobre los cambios que han aparecido en 2018 respecto a la protección de datos personales, para que tanto las personas como las empresas sepan de una manera sencilla, lo que tienen que hacer para cumplir la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Otro de los objetivos es ampliar mis conocimientos sobre las leyes de protección de datos ya que es algo muy a tener en cuenta, sobre todo en profesiones relacionadas con la informática, porque estas involucran datos personales en muchas ocasiones.

Y, por último, obtener los conocimientos necesarios para ser capaz de generar una lista de tareas pendientes con las características propias de una “to-do list” mediante la conocida herramienta software de hojas de cálculo Microsoft Excel.

1.2 Estructura

Este trabajo se divide en 4 secciones. La primera sección describe los cambios de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales respecto a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

La segunda sección describe el proceso llevado a cabo para el desarrollo de una lista con tareas pendientes realizada con software de hojas de cálculo.

La tercera contiene las conclusiones obtenidas tras el desarrollo del trabajo.

Y la última sección trata de una serie de anexos que proporcionan información adicional sobre: el delegado de protección de datos, la Agencia Española de Protección de Datos, la garantía de los derechos digitales, cambios en otras leyes, sanciones y prescripciones.

2. Cambios respecto a la LOPD

2.1 Datos de personas fallecidas

En la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, a diferencia de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, sí que se contempla el no tratamiento de datos personales de una persona fallecida.

Los herederos y familiares del fallecido pueden solicitar el acceso, rectificación y supresión de los datos, a no ser que una ley o el propio fallecido, lo hubiera prohibido expresamente. En ningún caso puede haber una prohibición sobre el derecho de acceso a los datos de carácter patrimonial a sus herederos.

También se especifican varios casos especiales:

- Si el fallecido es un menor, sus representantes legales y el Ministerio Fiscal tienen también derecho al acceso, rectificación y supresión de los datos personales del fallecido.

- Si el fallecido es un discapacitado, a la lista del caso anterior se le añaden las personas designadas a apoyarle, si dichas facultades estuviesen incluidas en las medidas de apoyo que puede realizar.

2.2 Principios de protección de datos

2.2.1 Exactitud de los datos

Los datos personales siempre deben ser exactos y en caso de que no lo sean, se deben rectificar o suprimir para asegurar la calidad de dichos datos. Esto es algo común en ambas leyes pero se añade una modificación, tal y como señala el artículo 4.2 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, que evita que el responsable del tratamiento sea acusado de un delito en relación a la inexactitud de los datos, en el caso de que dicho responsable haya tomado todas las medidas razonables para rectificar o suprimir la inexactitud de estos datos personales con respecto a los fines acordados cuando los hubiera obtenido directamente del afectado, de un intermediario, de un registro público o de otro responsable, cuando este último esté haciendo uso del derecho a la portabilidad mencionado en el artículo 20 del Reglamento (UE) 2016/679.

2.2.2 Deber de confidencialidad

El artículo 10, sobre el deber de secreto, de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 se sustituye por el artículo 5, sobre el deber de confidencialidad, de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Se mantiene el deber de secreto y se añade a todas las personas que intervengan en alguna fase del tratamiento de datos, incluyendo a los responsables y encargados del tratamiento, el deber de confidencialidad descrito en el artículo 5.1f del Reglamento (UE) 2016/679 de la siguiente forma:

> *Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("integridad y confidencialidad").*

2.2.3 Consentimiento del afectado

Deja de ser válido el consentimiento tácito, el cual permitía que en caso de silencio o inacción del afectado se realizase el tratamiento de los datos, y solo se aceptará un consentimiento libre, específico, informado e inequívoco por parte del afectado mediante una clara acción afirmativa o una declaración.

Es necesario que, si dicho tratamiento contiene varias finalidades, se informe al afectado de forma clara sobre cada una de ellas, de manera que el afectado sepa para que está dando su consentimiento.

El contrato no será válido para propósitos que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

En caso de que el afectado sea menor de catorce años, el tratamiento de sus datos personales solo podrá ser llevado a cabo con el consentimiento del titular de la patria potestad o tutela con el alcance determinado por el mismo.

Para que el tratamiento de los datos personales de un menor se pueda basar únicamente en el consentimiento de este, dicho afectado debe ser mayor de 14 años y no debe haber una ley que exija la asistencia de los titulares de la patria potestad o tutela en la celebración del acto en el que se recabe el consentimiento para el tratamiento.

2.2.4 Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos

La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 permite que se puedan llevar a cabo tratamientos de datos fundados en el cumplimiento de una obligación legal o en el interés público.

Se puede llevar a cabo un tratamiento de datos por obligación legal siempre que así lo considere una norma de Derecho de la Unión Europea o una norma con rango de ley, esta misma fijará las condiciones del tratamiento, los datos objeto de este y las cesiones de datos necesarias para el cumplimiento de la obligación legal.

Un tratamiento de datos personales podrá estar basado en el cumplimiento de una tarea realizada en interés público o para ejercer poderes públicos otorgados al responsable, cuando proceda de una competencia otorgada por una norma con rango de ley.

2.2.5 Categorías especiales de datos

Al conjunto de datos especialmente protegidos, que solo pueden ser tratados bajo determinadas circunstancias, se añaden los datos genéticos, los datos biométricos y los datos relativos a la salud.

Citadas textualmente del artículo 9.2 del Reglamento (UE) 2016/679, las circunstancias en las que se pueden tratar los datos especiales son las siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

e) El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3.

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, 4.5.2016 L 119/38 Diario Oficial de la Unión Europea ES.

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

No se permite el tratamiento de este tipo de datos en situaciones distintas a las mencionadas previamente y en caso de que suceda, se trataría de una infracción muy grave que supondría una gran sanción como se detalla en el Anexo B de este documento. Además, los tratamientos que se encuentren en alguna de las últimas tres situaciones citadas deben estar respaldados en alguna norma de rango ley que establezca condiciones sobre la seguridad y confidencialidad del tratamiento.

2.2.6 Tratamiento de datos de naturaleza penal

Con motivo de prevención, investigación y detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales se puede realizar el tratamiento de datos personales referentes a condenas, infracciones penales, procedimientos y medidas cautelares y de seguridad. Si el fin es distinto a los mencionados previamente, solo se podrán tratar estos datos cuando sea respaldado por una norma de Derecho de la Unión.

El registro completo de los datos de naturaleza penal se puede realizar según lo estipulado en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

Un abogado o procurador, con el fin de realizar su trabajo, puede llevar a cabo el tratamiento de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas.

2.3 Derechos del interesado

2.3.1 Transparencia e información al afectado

El responsable del tratamiento debe proporcionar, al afectado, información básica sobre el tratamiento de sus datos e indicarle un método de acceso a la información restante, ya sea mediante una dirección electrónica u otro medio.

En el caso de que los datos se hayan obtenido directamente del afectado, solo será necesario informarle de la identidad del responsable del tratamiento y de su representante, en caso de que lo tuviera, la finalidad del tratamiento y su posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación, portabilidad de los datos, oposición y decisiones individuales automatizadas, incluida la elaboración de perfiles.

Por otra parte, si los datos no se han obtenido por parte del afectado, también se le deberá informar de las categorías de datos objeto de tratamiento y las fuentes de las que proceden los datos.

2.3.2 Derecho de acceso

Tras el cambio de normativa, el afectado tiene derecho a obtener más información sobre sus datos personales y el tratamiento de estos, en concreto puede conocer los propósitos del tratamiento, las categorías de los datos personales, los destinatarios o categorías de destinatarios a los que se les va a comunicar sus datos, el plazo o criterio para la conservación de dichos datos, los derechos que puede aplicar en relación al tratamiento de sus datos personales, el origen de los datos en caso de que no los haya proporcionado él mismo e información sobre la existencia de decisiones automatizadas entre las que se incluye la elaboración de perfiles.

Para llevar a cabo el derecho de acceso, en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, el responsable del tratamiento le facilitaba al afectado un escrito con la información relativa al tratamiento de sus datos, sin embargo, en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, el responsable le proporciona al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice el acceso a los datos.

Además, la información mencionada en el primer párrafo de esta sección que no esté presente en el sistema de acceso remoto podrá ser solicitada por el interesado.

En la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, este derecho de acceso solo se podía realizar en intervalos mayores o iguales a 12 meses, salvo que se justificase un interés legítimo para ejercitarlo antes de que transcurra ese periodo de tiempo, en cambio, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 acorta el tiempo de espera entre solicitudes a 6 meses y no solo depende de la causa legítima, también depende de la decisión del responsable del tratamiento, exista o no una acreditación del interés legítimo por parte del interesado.

Tanto si el afectado elige un medio, que implique un coste desproporcionado, distinto al ofrecido por el responsable, como si el interesado pretende acceder reiteradamente (en intervalos menores a 6 meses) a sus datos sin acreditar un interés legítimo, el responsable puede cobrar un canon razonable en función de los costes producidos por estos dos casos.

2.3.3 Derecho de rectificación

Tanto en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, como en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, se atribuye al afectado un derecho para solicitar la modificación de los datos inexactos o incompletos que formen parte de un tratamiento de datos personales, pero la diferencia es que en esta última no hay un tiempo límite específico, ya que la ley de 1999 exigía al responsable del tratamiento cumplir este derecho en un plazo de 10 días y la ley de 2018 solo requiere que sea sin dilación indebida del responsable.

Además, la solicitud del afectado para que se lleve a cabo la rectificación deberá especificar los datos y la corrección que se tenga que realizar incluyendo, en caso de que fuera necesario, un documento que justifique la inexactitud o carácter incompleto de los datos del tratamiento.

2.3.4 Derecho al olvido

El derecho de supresión, también conocido como derecho al olvido, sustituye al derecho de cancelación descrito en el artículo 16 de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, el cual se encargaba de bloquear los datos y conservarlos únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, por si fueran necesarios hasta que prescriban las responsabilidades del tratamiento, después de esto se suprimen dichos datos.

El derecho al olvido exige al responsable del tratamiento que se encargue de cumplir este derecho del afectado sin dilación indebida cuando: no se requieran los datos personales para los fines acordados en el tratamiento, el interesado haya retirado su consentimiento y el tratamiento no se base en algún fundamento jurídico, los datos personales se hubieran tratado ilegalmente, el interesado haga uso del derecho de oposición y no predominen otros motivos legítimos para el tratamiento, se tengan que suprimir los datos personales para cumplir con una obligación legal aplicable al responsable del tratamiento, o los datos personales se hayan obtenido en relación con la oferta directa a niños de servicios de la sociedad de la información.

En caso de que los datos personales fueran públicos, el responsable debe tomar medidas razonables para informar a los responsables del tratamiento de esos datos de la solicitud de supresión de cualquier copia o enlace a los mismos.

No será aplicable la supresión de los datos personales cuando el tratamiento sea necesario para: hacer uso del derecho de libertad de expresión e información; cumplir una obligación legal del responsable para la cual se necesite el tratamiento de datos; cumplir una tarea de interés público o en el ejercicio de poderes públicos del responsable; formular, ejercer o defender reclamaciones; llevar a cabo fines de investigación o estadísticos que minimicen la exposición de datos personales de manera que no se permita identificar a los interesados.

2.3.5 Derecho a la limitación del tratamiento

Se añade un derecho para limitar tratamientos de datos personales, de manera que solo se pueda tratar para realizar procesos de reclamaciones, para proteger los derechos de otra persona, para cumplir tareas de interés público importante de la Unión o de algún Estado miembro, o para su conservación. No se podrán tratar los datos personales, que estén bajo una limitación, para otros fines salvo que el afectado de su consentimiento.

Estas limitaciones se llevan a cabo cuando: el responsable tenga que verificar la exactitud de los datos, por petición del afectado; el tratamiento sea ilegal y el interesado rechace la supresión de los datos y solicite la limitación de uso de los mismos; el interesado requiera los datos para realizar un proceso de reclamaciones, a pesar de que el interesado ya no necesite los datos para las finalidades del tratamiento acordadas o; cuando el interesado haga uso de su derecho de oposición al tratamiento, durante el periodo en el que se verifica si los motivos legítimos del responsable predominan sobre los del interesado.

Los sistemas de información del responsable deben registrar el hecho de que el tratamiento de datos personales esté limitado. Además, cuando se levante la limitación del tratamiento, el responsable ya debe habérselo notificado al interesado previamente.

2.3.6 Derecho a la portabilidad

La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 ofrece al interesado la posibilidad de obtener sus datos personales que hayan sido utilizados en algún tratamiento y dárselos a otro responsable del tratamiento, siempre y cuando este tratamiento se efectúe por medios automatizados y se base en el consentimiento del interesado o sea necesario para un contrato del cual forme parte el interesado. Así mismo, también puede solicitar que sus datos personales se transmitan de responsable a responsable siempre y cuando sea técnicamente posible.

Este derecho no debe afectar negativamente a los derecho y libertades de otros, ni ir en contra del derecho al olvido. Dicho derecho no se aplica en tratamientos necesarios para que se cumplan tareas relacionadas con el interés público o el ejercicio de los poderes públicos del responsable.

2.3.7 Derecho de oposición

El interesado puede oponerse a tratamientos de datos personales basados en el cumplimiento de una tarea de interés público, en el ejercicio de poderes públicos del responsable o la satisfacción de intereses legítimos del responsable o un tercero, exceptuando el caso de que el responsable justifique causas legítimas que predominen sobre los intereses, derechos y libertades del interesado, o para efectuar procesos relacionados con reclamaciones.

Si el objeto del tratamiento es la mercadotecnia directa, el afectado también puede oponerse al tratamiento de sus datos personales.

En caso de que el tratamiento tenga fines estadísticos o la investigación científica o histórica sea su objetivo, el interesado puede oponerse al tratamiento de sus datos a no ser que se requiera para el cumplimiento de una misión con motivos de interés público.

Este derecho de oposición debe haber sido comunicado al afectado de manera explícita y clara en el primer contacto con el responsable.

El interesado tiene derecho a no ser objeto de una decisión que le provoque efectos jurídicos o le afecte de manera significativa y se base exclusivamente en un tratamiento automatizado salvo que: el interesado haya dado su consentimiento explícito, sea necesaria para el ejercicio de un contrato entre el responsable y el interesado, o la autorice el Derecho de la Unión o de los Estados miembros aplicables al responsable. En estas 3 situaciones se deben tomar medidas que defiendan y aseguren los derechos, libertades e intereses legítimos del interesado.

2.4 Tratamientos concretos

2.4.1 Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales

Se puede llevar a cabo un tratamiento de datos de contacto de personas físicas que presten servicios en una persona jurídica si la única finalidad es establecer contacto con la persona jurídica y el tratamiento contiene solamente los datos necesarios para su localización profesional. Además, los intereses del responsable del tratamiento o de un tercero que quiera tratar estos datos no deben predominar sobre los intereses, derechos y libertades del afectado. Sucede lo mismo con el tratamiento de los datos referentes a empresarios individuales y profesionales liberales.

Cuando sea necesario para cumplir una obligación legal o ejercer sus competencias, los responsables citados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, también pueden realizar el tratamiento al que se refiere este apartado.

2.4.2 Sistemas de información crediticia

Para tratar lícitamente datos personales relacionados con el incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia se deben cumplir una serie de requisitos:

- El que proporcione los datos debe ser el acreedor o alguien que actúe por su cuenta o interés.

- Las deudas sean ciertas, vencidas, exigibles y el deudor no hubiera presentado una reclamación administrativa o judicial, ni se hubiera llegado un acuerdo entre el deudor y el acreedor.

- El acreedor haya notificado claramente al afectado la posibilidad de utilizar alguno de estos sistemas e indicarle cuales usará. La entidad que mantenga el sistema debe notificar al afectado la inclusión de sus datos e informarle sobre los derechos que puede ejercer (derecho de acceso, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y decisiones individuales automatizadas) en los 30 próximos días a la inclusión de sus datos en el sistema.

- Solo se mantendrán los datos en el sistema mientras perdure el incumplimiento y con una duración menor o igual a 5 años desde la fecha de vencimiento de la deuda.

- Solamente puedan consultar los datos de un deudor aquellos que hayan tenido una relación contractual con el mismo, en la que existan pagos, sobre todo si son mediante financiación, pago aplazado o facturación periódica. En caso de que el afectado hubiera presentado una solicitud para que se rectifiquen datos, el sistema debe indicar esta situación en el momento de la consulta y no mostrar los datos que se estén verificando hasta que se compruebe que son exactos.

- Si no se celebra el contrato o si se deniega, los que hayan consultado los datos en el sistema deben notificárselo al afectado.

Lo mencionado previamente en este apartado no contempla los supuestos en los que la información crediticia provenga de otras fuentes y se pretenda realizar un perfilado.

Las asociaciones que mantienen el sistema y las acreedoras son consideradas corresponsables, obteniendo así los derechos y responsabilidades que les corresponden.

2.4.3 Tratamientos relacionados con la realización de determinadas operaciones mercantiles

Para que puedan ser lícitos los tratamientos de datos derivados del desarrollo de una operación que realice cambios fundamentales en la organización y funcionamiento de sociedades mercantiles o la aportación o transmisión de negocio o de rama de actividad empresarial, dichos tratamientos deben ser necesarios para el buen fin de la operación y que aseguren la continuidad en la prestación de servicios.

Si no se concluye la operación, la entidad cesionaria debe suprimir los datos del tratamiento efectuado, de manera que no sea necesario aplicar la obligación de bloqueo.

2.4.4 Tratamientos con fines de videovigilancia

Cualquier persona física o jurídica puede utilizar sistemas de cámaras o videocámaras para tratar imágenes con el objetivo de mantener la seguridad de instalaciones, personas y sus bienes. Es posible captar imágenes en la vía pública cuando sea necesario para cumplir este objetivo o para asegurar bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, siempre y cuando no se tomen imágenes del interior de domicilios privados.

Los datos captados por este tipo de sistemas solo podrán almacenarse durante un mes, una vez transcurrido ese periodo de tiempo se deberán suprimir los datos, salvo que se haya captado alguna acción que vaya en contra de la integridad de personas, bienes o instalaciones. En este caso, se deberá facilitar las imágenes a la autoridad competente en menos de 72 horas desde el conocimiento del suceso.

A este tipo de tratamientos no se les podrá aplicar la obligación de bloqueo descrita en el artículo 32 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Para cumplir el deber de información al afectado es necesario colocar en un lugar visible un panel que contenga, como mínimo, información sobre la existencia del tratamiento de imágenes, la identidad del responsable y la posibilidad de hacer uso de los siguientes derechos: derecho de acceso, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos y derecho de oposición y decisiones individuales automatizadas.

Este reglamento no se aplica al tratamiento llevado a cabo por una persona física de imágenes que capten únicamente el interior de su domicilio, pero si se aplica al tratamiento llevado a cabo por una entidad de seguridad privada contratada para la vigilancia de un domicilio o que tenga acceso a las imágenes de este.

El tratamiento de datos obtenidos a través de este tipo de sistemas de vigilancia por parte del empleador tiene que cumplir el artículo 89, sobre el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

2.4.5 Sistemas de exclusión publicitaria

Cualquier persona puede oponerse a que le envíen comunicaciones comerciales y por ello, se considera lícito el tratamiento de datos personales, mediante sistemas de información en los que se registren únicamente los datos necesarios para identificar a todas estas personas. Estos sistemas también pueden incluir servicios de preferencia, que permitan a los afectados recibir publicidad de determinadas empresas.

Las empresas responsables de alguno de estos sistemas deben comunicar a la autoridad de control competente su creación, si es de carácter general o sectorial y el modo de incorporación de los afectados, así como la forma de establecer sus preferencias en caso de que dicho sistema ofreciera un servicio de preferencias.

La autoridad de control competente deberá encargarse de lo siguiente:

- Publicar en su página web una relación de estos sistemas que le hubieran comunicado, añadiendo la información facilitada por las empresas responsable descrita previamente.

- Comunicar al resto de las autoridades de control la información de estos sistemas para que también la publiquen en sus páginas web.

En caso de que un afectado le comunicase al responsable que no desea que sus datos sean tratados para fines publicitarios, este debe ofrecerle información sobre los sistemas de exclusión publicitaria existentes.

Salvo que el afectado ofrezca su consentimiento, los que pretendan realizar comunicaciones de mercadotécnica directa deben revisar los sistemas de exclusión publicitaria publicados por la autoridad de control competente, para no tratar datos de personas que se hayan negado a recibir comunicaciones comerciales.

2.4.6 Sistemas de información de denuncias internas

Es lícito el mantenimiento y creación de sistemas de información que contengan actos o conductas que puedan incumplir la normativa general o sectorial que se les aplique. Se debe informar sobre la existencia de estos sistemas a los empleados y terceros, a pesar de que únicamente tendrán acceso a los datos del sistema las siguientes personas:

- Las personas dedicadas al desarrollo de las funciones de control interno y de cumplimiento, o encargados del tratamiento asignados a estas tareas.

- Si fuera necesario para tomar medidas disciplinarias o para tramitar procedimientos judiciales podrán acceder también otras personas e incluso se permitirá la transmisión a terceros.

- El personal dedicado a la gestión y control de recursos humanos, cuando sea necesario tomar medidas disciplinarias contra un trabajador.

Es necesario que se adopten medidas para proteger la identidad y garantizar la confidencialidad de los datos sobre los afectados por la información introducida en este sistema.

Estos datos deben conservarse mientras se decide si iniciar o no una investigación sobre los hechos, como máximo se podrán mantener en el sistema durante 3 meses y tras esto se suprimirán los dados. a no ser que el objetivo sea dejar constancia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Los sucesos cuya denuncia no se haya iniciado, solo podrán permanecer en el sistema de forma anónima.

Una vez suprimidos del sistema, el órgano encargado de investigar los hechos denunciados podrá seguir tratando los datos con el objetivo de asegurar el cumplimiento de las normas, tomar medidas disciplinarias o tramitar procedimientos judiciales.

2.4.7 Tratamiento de datos relativos a infracciones y sanciones administrativas

El tratamiento de datos referente a infracciones y sanciones administrativas se debe limitar únicamente a los datos necesarios para cumplir su finalidad y los responsables de estos tratamientos serán los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

En el caso de que alguna de estas dos exigencias no se cumpla, se debe contar con el consentimiento del interesado o la autorización por parte de una norma de rango ley que regule garantías adicionales para los derechos y libertades de los afectados.

Además, los abogados y procuradores podrán llevar a cabo este tipo de tratamiento de datos cuando su objetivo sea recoger la información proporcionada por sus clientes para ejercer sus funciones.

2.5 Responsable y encargado del tratamiento

2.5.1 Obligaciones generales del responsable y encargado del tratamiento

Al igual que en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, los encargados y responsables del tratamiento deben decidir las medidas que hay que aplicar para garantizar y acreditar que el tratamiento cumpla la normativa de protección de datos. Con la diferencia de que ahora, también valorarán si es necesario realizar una evaluación de impacto en la protección de datos.

A la hora de definir estas medidas, los encargados y responsables del tratamiento deben tomar en consideración los riesgos que puedan producirse en los casos descritos, en el artículo 28.2 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, tal que así:

> *a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad*

de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

2.5.2 Supuestos de corresponsabilidad en el tratamiento

Aparece la figura del corresponsable, esta surge cuando varios responsables deciden conjuntamente los objetivos y medios del tratamiento. Las responsabilidades asociadas a cada corresponsable se determinan en función de las tareas que realizan, para asegurar un tratamiento de datos que no incumpla la normativa de protección de datos.

2.5.3 Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea

Cuando el tratamiento de datos personales lo lleve a cabo un responsable o encargado no establecido en la Unión Europea, las actividades del tratamiento sean el control de comportamientos o la oferta de bienes o servicios y tenga como afectado a un residente de la Unión, la Agencia Española de Protección de Datos o la correspondiente autoridad autonómica de protección de datos podrá imponer al representante las medidas establecidas en el Reglamento (UE) 2016/679.

En caso de incumplimiento de la normativa, los representantes, responsables y encargados del tratamiento tendrán que hacerse cargo de los daños ocasionados salvo que demuestren no ser responsables del hecho causante de estos daños.

2.5.4 Registro de las actividades de tratamiento

Uno de los cambios más relevantes respecto a la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 es la aparición del registro de actividades. Los representantes, responsables y encargados del tratamiento tienen la obligación de mantener un registro actualizado de las actividades aplicadas al tratamiento.

Los responsables y su representante (en caso de que lo tuvieran) se encargarán de realizar un registro de las actividades del tratamiento que se efectúen bajo su responsabilidad. Este registro contendrá la siguiente información:

- El nombre y los datos de contacto del responsable, del delegado de protección de datos, del representante del responsable y del corresponsable, en caso de que los hubiera.

- Los objetivos del tratamiento.

- Una descripción de las categorías de interesados, de las categorías de destinatarios a quienes se comunican los datos y de las categorías de los datos personales que aparecen en el tratamiento.

- La existencia de transferencias de datos personales a un tercer país o una organización internacional, información que permita identificar este país u organización, así como la documentación de garantías en caso de que fueran necesarias.

- Los plazos previstos, en la medida de lo posible, para la supresión de categorías de datos.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas realizadas, que garanticen la seguridad del tratamiento.

Los encargados y su representante (en caso de que lo tuvieran) se debe encargar de llevar un registro actualizado de todas las categorías de actividades de tratamiento que realice en nombre de un responsable. Este registro debe contener la siguiente información:

- El nombre y los datos de contacto de los encargados, de los responsables por los cuales haya actuado, del delegado de protección de datos y del representante del responsable o encargado, en caso de que los hubiera.

- Las categorías de tratamientos efectuados en nombre de cada responsable.

- La existencia de transferencias de datos personales a un tercer país o una organización internacional, información que permita identificar este país u organización, así como la documentación de garantías en caso de que fueran necesarias.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas realizadas, que garanticen la seguridad del tratamiento.

La obligación de llevar los registros mencionados no será aplicable a empresas u organizaciones que tenga menos de 250 empleados, salvo que el tratamiento pueda suponer un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos personales o datos personales relacionados con condenas e infracciones penales.

Las entidades mencionadas en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos que contenga la información incluida en estos registros y las bases legales.

2.5.5 Bloqueo de los datos

En la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, solo se realizaba el bloqueo de datos tras una cancelación, sin embargo, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 exige al responsable del tratamiento que también bloquee los datos durante la rectificación de los mismos.

Los datos bloqueados solo podrán ser tratados para proporcionárselos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes con objeto de exigir responsabilidades referentes al tratamiento. Cuando prescriban estas responsabilidades, no podrán ser exigidas y los datos deberán ser destruidos.

En el caso de que sea necesario realizar un bloqueo de datos, pero el sistema no lo permita o se requiera un esfuerzo desproporcionado, se hará una copia segura de la información que se vaya a bloquear. Esta copia incluirá la fecha del bloqueo, servirá como evidencia digital y asegurará que la información es auténtica y que no se han manipulado los datos.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos pueden añadir excepciones a esta obligación de bloqueo cuando la conservación de los datos pueda suponer un alto riesgo para los derechos de los afectados, ya sea porque hay demasiados afectados o por la propia naturaleza de los datos que se tratan, y también cuando la conservación de los datos pueda implicar un coste desproporcionado para el responsable.

2.5.6 Encargado del tratamiento

Los encargados pueden acceder a los datos personales necesarios para prestarle un servicio al responsable, sin que se considere comunicación de datos siempre y cuando cumpla el Reglamento (UE) 2016/679, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y las normas de su desarrollo.

Tienen también, la posibilidad de conservar los datos referentes a las responsabilidades de su relación con el responsable, asegurándose que estos datos estén bloqueados.

Un órgano de la Administración General del Estado, la Administración de comunidades autónomas, las Entidades que integran la Administración Local o los Organismos vinculados o dependientes podrán ejercer de encargados en el ámbito del sector público siempre y cuando se

adopte una norma que regule las competencias atribuidas. Esta norma debe integrar lo dispuesto en el artículo 28.3 del Reglamento (UE) 2016/679.

Si un encargado establece relaciones con los afectados actuando bajo su propio nombre, salvo que se efectúe en el marco de la legislación de contratación del sector público, será considerado como responsable del tratamiento. Así mismo, al igual que en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, se le considerará responsable si utiliza los datos para sus propias finalidades.

2.5.7 Guía de actuación del encargado ante los nuevos derechos

El encargado del tratamiento no toma decisiones sobre el uso de la información o la finalidad del tratamiento, pero sí que se encarga de registrar todas las actividades de tratamiento que realice, de cooperar con la autoridad de control que lo solicite, de tomar las medidas de seguridad adecuadas para el tratamiento, de notificar al responsable todas y cada una de las violaciones de seguridad que conozca y además, debe realizar todas las tareas descritas en el contrato que tiene con el responsable del tratamiento.

En este apartado se detallan las tareas y los pasos a seguir para que el encargado pueda realizarlas correctamente. Estas tareas son las siguientes:

a) Documentar: Los motivos principales para documentar todo lo relativo al tratamiento de datos y su seguridad son: cumplir lo exigido por la ley sobre el registro de las actividades de tratamiento de datos, que se trata en el apartado “2.5.4 Registro de las actividades de tratamiento” de este documento, poder utilizar la información para sacar conclusiones en el futuro y evitar el riesgo de perder toda esa valiosa información en caso de que haya un cambio de encargado. Puesto que en la bitácora todo debe estar ordenado cronológicamente, es recomendable anotarlo todo nada más suceda para evitar el riesgo de que se te olvide algo. Se debe dejar constancia de: todas las actividades de tratamiento que se realizan; los accesos e incidentes, así como toda la información referente a estos, incluyendo las acciones tomadas para gestionar los incidentes; los usuarios y equipos existentes; las transmisiones de datos realizadas y los destinatarios; la gestión de copias de seguridad y; del aprendizaje y las dificultades encontradas durante las actividades.

Si se utiliza un bloc en papel, es recomendable dejar aproximadamente 5 hojas en blanco después de la portada para tener sitio para la tabla de contenidos, porque como es un documento que se va rellenando con el tiempo, esta tabla se ampliará constantemente.

Debido a la importancia de esta información, cada vez que pare de utilizar la bitácora, en caso de que esté redactada en papel es necesario almacenarla en un lugar seguro, y si se redacta en formato digital asegurarse de que esté bien protegido.

b) Copias de seguridad: La gestión de las copias de seguridad es importante para asegurar la integridad de los datos que se tratan, ya sea para proporcionárselos a las autoridades en caso de que los necesiten, para poder restaurar los datos originales en caso de que ocurra algún incidente o para cualquier otra situación que pueda darse. Antes que nada, hay que decidir en qué tipos de dispositivos se van a almacenar las copias de seguridad, teniendo en cuenta las ventajas y desventajas que presenta cada dispositivo y priorizando, ante todo, la seguridad de las copias. Se

aconseja utilizar la “regla 3-2-1” que consiste en crear 3 copias diariamente, siempre que sea posible y haya datos nuevos o modificados, almacenar las copias en 2 medios distintos y que 1 de las copias esté alojada en un sitio físico diferente. En caso de optar por el almacenamiento en la nube, es altamente recomendable que apliques un cifrado a las copias para aumentar el nivel de seguridad de los datos.

Se recomienda realizar pruebas con bastante regularidad (una vez a la semana como mínimo) para asegurarse de que sea posible restaurar las copias de seguridad, de esta manera, cuando realmente sea necesario llevar a cabo la restauración, no habrá ningún problema inesperado. Estas pruebas no se deben realizar sobre el soporte que contiene los datos originales, puesto que como su propio nombre indica, son simplemente pruebas y por ello se deben tratar como una simulación, no como un caso real.

El borrado de datos o la destrucción de dispositivos de almacenamiento es algo bastante común ya que ni el tratamiento de datos es permanente, ni la vida de los soportes de información es infinita y, por lo tanto, hay que saber actuar en caso de que sea necesario llevarlo a cabo. No es suficiente con eliminar los archivos o formatear el dispositivo con las herramientas que ofrece el propio sistema operativo, hay que realizar un borrado seguro que no permita recuperar los datos “eliminados”. Antes que nada, hay que decidir el método de destrucción de la información (desmagnetización, destrucción física o sobre-escritura), en función del tipo de dispositivo en el que se almacena la información y de las ventajas e inconvenientes que presenta cada método. Debido a la cantidad de ventajas que presenta la sobre-escritura es altamente recomendable usar este método excepto para dispositivos que estén dañados o dispositivos ópticos o no regrabables, ya que este método consiste en escribir datos en la totalidad de la superficie de almacenamiento. Para más información sobre estos métodos, puedes acceder a la guía sobre borrado seguro del Instituto Nacional de Ciberseguridad a través de su página web.

Instituto Nacional de Ciberseguridad: Guía sobre borrado seguro de la información. Incibe, 2016. Fecha del último acceso: 3 de septiembre de 2019. [Disponible en: www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad_0.pdf]

c) Gestión de incidencias: Debido al riesgo que suponen, es necesario llevar a cabo un seguimiento de los incidentes. Para ello, se deben realizar frecuentemente una serie de tareas que se mencionan a continuación.

Primero se inicia una fase de detección, que comienza con el uso de los mecanismos de detección o sistemas de alerta seleccionados por el responsable, para detectar los incidentes. Una vez obtenida la información a través de estas herramientas, se analiza esta información. Tras el análisis, se habrá identificado si es un incidente de seguridad y si ha afectado a datos de carácter personal, entre otros aspectos. Es importante registrar estos incidentes incluyendo el tipo de incidente, la descripción, la gravedad, el estado y las medidas tomadas para resolverlo.

Tras finalizar la fase de detección, se inicia una etapa de clasificación, en la cual primero se determinar el tipo al que pertenece el incidente. Después se realiza una valoración del alcance de la brecha de seguridad, en la cual hay que tomar en consideración aspectos como el impacto de la brecha, el número de afectados, la categoría de la brecha y el volumen de datos, entre otros.

A continuación, se lleva a cabo el plan de actuación cuyo primer paso es iniciar el proceso de respuesta. Se deben tomar las medidas necesarias para contener el incidente. Después, se aplican tareas de erradicación para solucionar los efectos provocados por el incidente. Al terminar de aplicar estas tareas, es necesario asegurarse de que hayan servido para erradicar el incidente. Se restablece el servicio para que vuelva a tener un funcionamiento normal. Para reducir el riesgo y evitar que vuelva a suceder un incidente con la misma causa, a corto y medio plazo, se identifican y analizan las posibles soluciones. Otro paso importante es seleccionar la estrategia que se llevará a cabo en el futuro, en función del riesgo, la eficiencia y los costes de las posibles opciones. Para posteriormente sacar conclusiones y poder comunicarlo a las partes interesadas, es necesario documentar el proceso de respuesta. Para finalizar la fase de resolución, se elabora un informe lo más completo posible que contenga, como mínimo, información sobre el alcance e impacto del incidente, los controles preventivos, las acciones tomadas para resolver de la brecha, las acciones preventivas para evitar futuras brechas, el impacto de las acciones de respuesta y las acciones definidas para el seguimiento.

Se debe notificar sin dilación indebida al responsable del tratamiento de las incidencias y brechas de seguridad en el plazo acordado en el contrato existente entre ambas partes, es recomendable que sea inferior a 72 horas. Además, se pueden dar dos situaciones distintas en función de si el responsable ha delegado en el encargado la obligación de notificar a los afectados y a las autoridades de control. Si no existe esta delegación, el encargado simplemente debe notificarle al encargado lo sucedido, recomendándole un proceso a seguir para llevar a cabo estas notificaciones a la autoridad de control y a los afectados, pero en caso de que exista la delegación el encargado debe realizar lo que se describe a continuación respecto a las notificaciones.

En caso de que el incidente sea clasificado como una brecha de seguridad que conlleve un riesgo para los derechos y libertades de las personas físicas, se inicia un proceso de notificación a la autoridad de control competente. El primer paso es desarrollar un informe que contenga: los datos identificativos y de contacto del responsable, el encargado y el delegado (cuando proceda); el tipo de notificación; fecha, hora y duración del incidente; fecha y hora de detección de la brecha; contenido, naturaleza y categoría de los datos afectados; resumen del incidente causante de la brecha; posibles consecuencias en los afectados; medidas llevadas a cabo; categoría y cantidad de individuos afectados e; implicaciones transfronterizas. Después hay que notificar el informe sin dilación indebida, de ser posible en menos de 72 horas. Si la autoridad de control principal es la Agencia Española de Protección de Datos, esta notificación se realiza a través del siguiente enlace: https://sedeagpd.gob.es/sede-electronica-web/. Cuando haya información requerida por el informe que no se conozca en ese plazo, se debe indicar en la primera notificación, que más adelante se proporcionará la información faltante. Todas estas notificaciones enviadas deben quedar registradas para poder demostrar el cumplimiento de notificación ante las autoridades de control.

Respecto a la notificación a los afectados, primero hay que analizar si debe notificar a los afectados, tomando en consideración las obligaciones legales y contractuales, los riesgos que conlleve la pérdida de los datos, la existencia de riesgos de fraude o suplantación de identidad y la posibilidad del afectado para disminuir o evitar posibles daños futuros. Después, estudiar si la comunicación al afectado supone algún obstáculo en alguna investigación en marcha. En caso afirmativo, pedir permiso a la autoridad de control para postponer esta notificación. Tras esto, se redacta un documento que contenga, al menos, los datos de contacto del Delegado de Protección de Datos, los detalles generales del incidente, las consecuencias que podría causar la brecha de

seguridad, la reseña de los datos afectados, las medidas relacionadas con el incidente llevadas a cabo y toda la información útil para la protección de los datos del afectado y la prevención de posibles daños. Una vez redactado el documento, se envía de forma directa, con la mayor brevedad posible, a través de alguno de los medios adecuados. Si la notificación directa supone un coste excesivo o no es posible contactar directamente con el afectado, se realizará una notificación indirecta.

Por último, se lleva a cabo una fase de seguimiento y cierre, en la cual hay que considerar si se debe contratar a un experto forense para la realización de un análisis forense digital. También hay que analizar que riesgos y consecuencias traería la aplicación de medidas procesales. Tras el análisis, en caso de que dichas medidas no resultasen contraproducentes, se iniciará un procedimiento judicial. Después, se comprueba si las medidas correctoras aprobadas son adecuadas para resolver la brecha de seguridad y para minimizar el riesgo cuando se produzcan casos similares. Y finalmente se redacta y se archiva un informe completo sobre la brecha.

d) Medidas de seguridad: Antes que nada, hay que evaluar los posibles riesgos producidos por el tratamiento. Tras haber realizado la evaluación y teniendo claro cada uno de los riesgos, se rellena una lista con las medidas de seguridad que se consideren oportunas. El encargado no solo tiene que realizar estas medidas, sino que también ha de revisar el contrato con el encargado, ya que en este acuerdo se encuentran las medidas de seguridad que establece el responsable.

Además de estas medidas de seguridad, debe adherirse a códigos de conducta u obtener certificados de entidades acreditadas para demostrar el cumplimiento de las medidas seleccionadas.

e) Subcontratación: En el contrato realizado entre el responsable y el encargado se debe tratar la autorización para que el encargado pueda contratar a otro encargado. Esta autorización por parte del responsable puede ser general o especificar la entidad determinada que pueda ser subcontratada. En caso de que no se haya especificado una entidad concreta, primero es necesario realizar un listado de los posibles candidatos, después seleccionar el candidato que mejor convenga (no se debe seleccionar un candidato que no ofrezcan las garantías apropiadas) y finalmente informar al responsable de la contratación que vaya a realizar el encargado para obtener su aprobación. Tras contar con la aprobación del responsable, hay que contactar al candidato seleccionado y hacer un contrato que le otorgue las mismas condiciones que tiene el encargado en lo que respecta al tratamiento de datos personales y a la garantía de derecho de los afectados.

Una vez finalizada la contratación, es altamente recomendable revisar que el subencargado desempeñe correctamente sus tareas y obligaciones, ya que el encargado inicial es responsable, de cualquier incumplimiento del subencargado, ante el responsable del tratamiento.

f) Derechos de los interesados: Antes de realizar cualquier tarea relacionada con las solicitudes de los afectados para hacer uso de sus derechos sobre el tratamiento, se verifica si en el contrato con el responsable se le asigna al encargado la tarea de atender y dar respuesta estas solicitudes o simplemente debe informar al responsable de que se ha ejercido el derecho. El segundo paso es enviar la notificación al responsable, dependiendo del caso, con una resolución u otra. En el primer caso, en el acuerdo con el responsable estarán estipulados los plazos y la forma de atender las solicitudes de ejercicio de estos derechos. En el segundo caso, en el acuerdo estarán

estipulados los plazos, la forma de atender las solicitudes y la información que debe comunicarle al responsable.

g) Colaboración con el responsable y las autoridades: Es importante revisar a diario el medio de comunicación establecido, generalmente correo electrónico, para comprobar si hay mensajes del responsable o de alguna autoridad de control. Además, para cumplir el deber de colaboración no solo tiene que esperar a recibir mensajes, si no que cuando sea preciso ofrecer ayuda el encargado será quien se ponga en contacto con ellos.

El método de proceder tras la comunicación no puede ser descrito en este apartado, ya que depende de muchísimos factores, pero se recomienda que haga todo lo posible por ayudarles en el cumplimiento de sus obligaciones.

h) Proceso final de la prestación de servicio: Este proceso se lleva a cabo una única vez por tratamiento, como es evidente, ya que solo se va a realizar cuando finalice la prestación de los servicios de tratamiento de datos. Hay dos formas de proceder dependiendo de lo descrito en el contrato con el responsable: la primera es devolver los datos y sus copias al responsable o al nuevo encargado del tratamiento y la segunda es eliminar los datos. En ambos casos, se aconseja que el encargado se quede con una copia de los datos siempre y cuando esté bloqueada correctamente. El proceso de borrado seguro se describe en el último párrafo del apartado 2.5.7.b de este documento. Cabe recalcar que si existe una obligación legal que exige la conservación de los datos, tendría que devolverlos al responsable para que se encargue de garantizar su conservación.

2.5.8 Designación de un delegado de protección de datos

Cualquier responsable o encargado tiene la posibilidad de designar voluntariamente un delegado de protección de datos, que cumpla el Reglamento (UE) 2016/679 y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, pero están obligados aquellos responsables o encargados de tratamientos cuyas actividades principales requieran una observación habitual y sistemática de interesados a gran escala, o consistan en el tratamiento a gran escala de categorías especiales de datos personales o datos referentes a condenas e infracciones penales, o cuando alguna de las siguientes entidades sea la que realiza el tratamiento:

- Autoridades u organismos públicos, excepto los tribunales que actúen en ejercicio de su función judicial.

- Los colegios profesionales y sus consejos generales.

- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación.

- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala

perfiles de los usuarios del servicio.

- Los bancos, las cajas de ahorros, las cooperativas de crédito o el Instituto de Crédito Oficial.

- Los establecimientos financieros de crédito.

- Las entidades aseguradoras y reaseguradoras.

- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Las entidades que desarrollen actividades de publicidad y prospección comercial cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de estos.

- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, exceptuando los profesionales de la salud que ejerzan su actividad a título individual.

- Las entidades que tengan como uno de sus fines la emisión de informes comerciales que puedan referirse a personas físicas.

- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

- Las empresas de seguridad privada.

- Las federaciones deportivas cuando traten datos de menores de edad.

El responsable o encargado que vaya a realizar la selección del delegado tiene que asegurarse de que el candidato reúna las cualidades necesarias para cumplir con las tareas y obligaciones del Delegado de Protección de Datos. Estas cualidades profesionales se describen en el Anexo E de este documento, concretamente en el apartado 9.1.

En caso de que el delegado seleccionado sea de la organización del responsable o encargado del tratamiento, ninguno de estos puede sancionarlo ni removerlo por el simple hecho de cumplir con sus funciones, salvo en casos de estafa o negligencia grave por parte del delegado.

La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos deben mantener un listado actualizado de los delegados de protección de datos, en el ámbito que les corresponda, que sea accesible por medios electrónicos. Para que puedan llevar a cabo este listado, es obligatorio que los responsables y encargados del tratamiento les comuniquen en un plazo máximo de 10 días las designaciones, nombramientos y ceses de los delegados de protección de datos.

Para información más detallada sobre el Delegado de Protección de Datos, se recomienda buscar el Anexo E de este documento.

2.6 Códigos de conducta

Los códigos de conducta son documentos redactados con la finalidad de ayudar a que se aplique correctamente el reglamento de protección de datos. En la antigua normativa de protección de datos, los códigos de conducta se denominaban códigos tipo, pero no son exactamente lo mismo ya que presentan una serie de diferencias. Una de las diferencias que presentan los códigos de conducta es su flexibilidad, ya que tal y como comentó Jesús Rubí Navarrete en una jornada informativa celebrada en la sede del Grupo PSN sobre la normativa de protección de datos personales, para que los códigos tipo tuvieran un elevado valor añadido se exigía que se incluyesen todas las actividades de tratamiento de un determinado sector, mientras que los códigos de conducta pueden estar limitados a determinadas actividades sectoriales o a la garantía del ejercicio de determinados derechos. Otra de las grandes diferencias es la aparición del principio de responsabilidad proactiva, el cual añade cierta obligatoriedad en el uso de los códigos ya que, a pesar de ser de carácter voluntario, si ocurriese algún problema daría lugar a sanciones muy elevadas por no haber aplicado un código, aprobado por la Agencia Española de Protección de Datos o la autoridad autonómica de protección de datos correspondiente, que demuestre el correcto cumplimiento de la normativa de protección de datos.

Todos los que acepten el código de conducta deberán acatar lo mencionado en dicho código y se verán obligados a poner en manos de la entidad de supervisión las reclamaciones sobre el tratamiento de datos presentadas por el afectado, cuando consideren que no procede atender a lo solicitado, siempre y cuando no vaya en contra de lo dispuesto en el artículo 37, sobre la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos, de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018. También pueden someter a la entidad de supervisión a que verifique si el tratamiento es adecuado con lo dispuesto en el código de conducta.

El papel que toma la Agencia Española de Protección de Datos respecto a los códigos de conducta es el de: animar a que se elaboren códigos de conducta; aprobarlos; mantener un registro de los códigos de conducta aprobados, que esté interconectado con los de registros de las autoridades autonómicas de protección de datos y coordinado con el registro del Comité Europeo de Protección de Datos; someter un proyecto de código de conducta al mecanismo de coherencia, cuando esté relacionado con un tratamiento de datos en distintos Estados miembros de la Unión y; actuar como intermediaria en las comunicaciones con el Comité Europeo de Protección de Datos asistida por un representante de la Autoridad autonómica, en caso de que sea la autoridad autonómica de protección de datos quien haya sometido el proyecto al mecanismo de coherencia.

Se pueden encontrar ejemplos de códigos de conducta en la página web de la Agencia Española de Protección de Datos, en concreto, el listado de códigos de conducta se encuentra en este enlace: https://www.aepd.es/reglamento/codigos-de-conducta/.

Las autoridades autonómicas de protección de datos también pueden (para casos del ámbito que les correspondan) aprobar códigos de conducta, mantener un registro de los que han aprobado y someter un proyecto de código de conducta al mecanismo de coherencia para tratamientos en distintos Estados miembros de la Unión.

Los códigos de conducta pueden ser promovidos por:

- Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento.

- Entidades que realicen funciones de supervisión y resolución extrajudicial de conflictos.

- Empresas o grupos de Empresas.

- Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

- Los órganos jurisdiccionales.

- La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

- Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

- Las autoridades administrativas independientes.

- El Banco de España.

- Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

- Las fundaciones del sector público.

- Las Universidades Públicas.

- Los consorcios.

- Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2.7 Acreditación de instituciones de certificación

La Entidad Nacional de Acreditación puede encargarse de acreditar a los organismos de certificación que posean mucha experiencia sobre protección de datos, sin afectar a las funciones y poderes de las autoridades de control competentes. Esta entidad también se encarga de comunicar su motivación y las concesiones, denegaciones y revocaciones de las acreditaciones a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas.

2.8 Transferencias internacionales de datos

La Ley Orgánica de Protección de Datos de Carácter Personal de 1999 exigía que, salvo excepciones o que se cumplieran las garantías adecuadas, no se pudiesen transferir datos a países que no cuenten con el mismo nivel de protección. Esa ley era bastante breve, con lo cual tampoco garantizaba un nivel muy alto de protección y sus exigencias eran más sencillas de cumplir, pero con la aparición de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, aumentaron las condiciones necesarias para asegurar el nivel de protección de datos personales.

Las transferencias internacionales de datos están sujetas a lo dispuesto en el Reglamento (UE) 2016/679, en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y sus normas de desarrollo aprobadas por el gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos.

La Agencia Española de Protección de Datos puede adoptar cláusulas contractuales tipo para la realización de transferencias internacionales de datos que deben haber sido previamente sometidas al dictamen del Comité Europeo de Protección de Datos, además, también puede aprobar normas corporativas vinculantes. Este procedimiento se inicia a petición de una entidad situada en España y queda suspendido hasta que el Comité Europeo de Protección de Datos emita el dictamen y lo notifique a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos correspondiente. La duración máxima del procedimiento es de 9 meses.

Las transferencias internacionales de datos a un país tercero o a una organización internacional deben contar con una decisión de adecuación aprobada por la Comisión o estar amparadas en alguna de las garantías comentadas previamente. En caso de que no se cumplan estas condiciones solo se podrá llevar a cabo la transferencia teniendo una autorización de la Agencia de Protección de Datos o de las autoridades autonómicas de protección de datos correspondientes. Dicha autorización solo se puede otorgar cuando la transferencia busque basarse en la aportación de garantías adecuadas con el fundamento en cláusulas contractuales no correspondientes a las cláusulas tipo o cuando la transferencia se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados y sea llevada a cabo por alguno de los siguientes encargados o responsables:

- Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

- Los órganos jurisdiccionales.

- La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

- Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

- Las autoridades administrativas independientes.

- El Banco de España.

- Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

- Las fundaciones del sector público.

- Las Universidades Públicas.

- Los consorcios.

- Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

La duración máxima del procedimiento mencionado es de 6 meses y dicha autorización tiene que ser sometida a la emisión de un dictamen realizado por el Comité Europeo de Protección de Datos.

Salvo que se refiera a las actividades llevadas a cabo por autoridades públicas en el ejercicio de sus poderes públicos, los responsables del tratamiento tienen la obligación de informar, a la Agencia Española de Protección de Datos o a las autoridades autonómicas de protección de datos, de las transferencias internacionales que vayan a realizar sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por los responsables y la concurrencia de los siguientes requisitos: la transferencia no sea repetitiva, solo afecte a un número limitado de interesados y el responsable del tratamiento evalúe todas las circunstancias concurrentes en la trasferencia de datos.

También es necesario que los responsables informen a los afectados sobre la transferencia y los intereses legítimos imperiosos perseguidos.

2.9 Agencias Española de Protección de datos

La Agencia Española de Protección de Datos cumple un papel muy importante en lo referente a la protección de datos personales en España y, por lo tanto, en este documento se le dedica un anexo bastante extenso (el Anexo D).

Se encarga de realizar unas funciones que deben conocer los responsables y encargados del tratamiento, puesto que les afectan. Una de estas funciones es la realización de investigaciones para asegurarse de que se cumple el vigente reglamento de protección de datos.

Pueden regular los tratamientos que llevan a cabo los encargados, así como imponer obligaciones a nuevos encargados.

Además, la Agencia Española de Protección de Datos ofrece asesoramiento a los responsables y encargados, en materia de las operaciones de alto riesgo y facilita una lista de este tipo de operaciones para que sepan cuando es necesario llevar a cabo una evaluación de impacto.

Este apartado es un resumen breve de lo que más afecta directamente a los responsables y encargados del tratamiento de datos, para una información más detallada de la Agencia Española de Protección de Datos se recomienda revisar el Anexo D previamente mencionado.

2.10 Autoridades autonómicas de protección de datos

Las autoridades autonómicas de protección de datos tienen las funciones y poderes descritos en el Anexo D, concretamente en los apartados 8.2 y 8.3, sobre funciones y poderes de la agencia española de este documento, exceptuando la función de publicidad, para los tratamientos:

- Realizados por personas, tanto físicas como jurídicas, en el ejercicio de cargos públicos dentro de la jurisdicción de su Administración Autonómica o Local.

- Dispuestos en sus Estatutos de Autonomía.

- Cuya responsabilidad recaiga sobre las entidades pertenecientes al sector público de su Comunidad Autónoma o de las Entidades Locales situadas en su ámbito territorial, o sobre quien preste servicios mediante cualquier modo de gestión directa o indirecta.

A parte de estas funciones y poderes, también pueden dictar circulares para los tratamientos que le correspondan, de igual alcance y efectos que las “Circulares de la Agencia Española de Protección de Datos”.

En la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, el director de la Agencia de Protección de Datos citaba con frecuencia a los órganos correspondientes de las Comunidades Autónomas para realizar un intercambio recíproco de información necesaria para el cumplimiento de sus funciones, tras el cambio de normativa de protección de datos, es la Presidencia de la Agencia Española de Protección de Datos quien convoca a las autoridades autonómicas de protección de datos para este tipo de cooperación y para contribuir a que se aplique, tanto el Reglamento (UE) 2016/679 como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

2.10.1 Tratamientos contrarios al reglamento (UE) 2016/679

Si la Agencia Española de Protección de Datos detecta que un tratamiento que competa a alguna autoridad autonómica incumple el reglamento europeo de protección de datos personales, le comunicará las medidas que deben llevar a cabo en el plazo de un mes para el cese del tratamiento ilícito. En caso de que no se lleven a cabo esas medidas en el plazo acordado o no cese el tratamiento ilícito, la Agencia Española de Protección de Datos tomará las acciones legales que considere necesarias.

2.10.2 Coordinación en comunicaciones con el Comité Europeo de Protección de Datos

La Agencia Española de Protección de Datos actúa como intermediaria entre las autoridades autonómicas de protección de datos y el Comité Europeo de Protección de Datos, cuando las autoridades autonómicas de protección de datos:

- necesiten someter su proyecto al Comité Europeo de Protección de Datos.

- soliciten un dictamen, en materia de protección de datos, del Comité Europeo de Protección de Datos.

- requieran una decisión para la resolución de conflictos por parte del Comité Europeo de Protección de Datos.

Las autoridades autonómicas interesadas no principales, para la resolución de conflictos del Comité, deben facilitar todo lo necesario a la Agencia Española de Protección de Datos.

Para llevar a cabo estas tareas, la Agencia Española de Protección de Datos cuenta con la asistencia de un representante de la Autoridad autonómica correspondiente.

2.10.3 Intervención en tratamientos transfronterizos

Cuando el tratamiento sea alguno de los mencionados al inicio del apartado 2.10, sobre las Autoridades Autonómicas de Protección de Datos, de este documento, las autoridades autonómicas de protección de datos correspondientes actuarán como autoridad de control principal en la cooperación con el resto de autoridades de control descrita en el Reglamento (UE) 2016/679.

Bajo esta consideración, las autoridades autonómicas participarán en las tareas mencionadas en el artículo 60 del Reglamento (UE) 2016/679 e informarán a la Agencia Española de Protección de Datos cuando sea necesario aplicar el mecanismo de coherencia.

2.11 Procedimientos en las posibles vulneraciones de la normativa de protección de datos

El procedimiento sancionador es uno de los grandes cambios sucedidos en la normativa de protección de datos, ya que en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 apenas se trataba en un breve artículo que mencionaba la duración de los procedimientos sancionadores y la vía por la cual se llevaban a cabo, sin embargo, en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 hay varios artículos que tratan el tema con mayor nivel de detalle.

El contenido de este apartado se aplica a los procedimientos en los que un afectado reclame que no se ha atendido su solicitud para ejercer con sus derechos sobre el tratamiento de datos

(derecho de acceso, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y decisiones individuales automatizadas) o en los que la Agencia Española de Protección de Datos investigue la existencia de un posible incumplimiento de la normativa de protección de datos.

Estos procedimientos son gestionados por la Agencia Española de Protección de Datos y regulados por el Gobierno, con el objetivo de asegurar a los interesados sus derechos de defensa y audiencia.

2.11.1 Inicio y duración del procedimiento

En las tablas 1 y 2 se describe tanto la forma de iniciación como la duración del procedimiento en función de la causa del procedimiento.

Tabla 1. Procedimiento por falta de atención. Fuente: LOPDGDD.

Motivo	Falta de atención de la solicitud del afectado para ejercer sus derechos sobre el tratamiento.
Forma de inicio	Acuerdo de admisión a trámite.
Plazo de resolución	6 meses desde la notificación al afectado sobre el resultado del acuerdo de admisión a trámite.

Tabla 2. Procedimiento por posible infracción. Fuente: LOPDGDD.

Motivo	Posible existencia de una infracción en la normativa de protección de datos.
Forma de inicio	Acuerdo de inicio por iniciativa propia.
	Acuerdo de inicio por consecuencia de una reclamación. Previamente, la Agencia Española de Protección de Datos debe decidir su admisión a trámite.
	Adopción de acuerdo de inicio de procedimiento sancionador, cuando deban aplicarse las normas correspondientes a la cooperación entre autoridades de control.
Información adicional	Antes del acuerdo de inicio, es posible llevar a cabo una fase de actuaciones previas de investigación.
Plazo de resolución	9 meses desde el acuerdo de inicio.

Todo lo dispuesto en estas dos tablas, exceptuando la previa decisión de la admisión a trámite de la segunda tabla, se aplica también en el caso de que la Agencia Española de Protección de Datos sea la autoridad de control principal del tratamiento y alguna autoridad de control de otro Estado miembro de la Unión Europea le haya comunicado una reclamación.

Cuando sea necesario obtener información o asistencia de alguna autoridad de control de los Estados miembros o de un órgano u organismo de la Unión Europea, se suspenderán los plazos de los procedimientos en las posibles vulneraciones de la normativa de protección de datos. La suspensión comienza en el inicio de la solicitud y finaliza cuando la Agencia Española de Protección de Datos recibe la notificación.

2.11.2 Admisión a trámite de las reclamaciones

Al recibir una reclamación, la Agencia Española de Protección de Datos debe determinar su admisibilidad a trámite. Se inadmiten las reclamaciones cuando sucede alguna de las siguientes condiciones:

- No tratan sobre protección de datos personales.

- No tienen fundamento.

- Son abusivas.

- No presentan indicios que den a entender que se pueda estar cometiendo una infracción.

- El responsable o encargado del tratamiento, antes de recibir la advertencia de la Agencia Española de Protección de Datos, ya haya tomado medidas para solucionar el posible incumplimiento de la normativa de protección de datos y no se haya causado daño al afectado en infracciones leves o el derecho del afectado esté completamente garantizado por la aplicación de estas medidas.

Además, la Agencia Española de Protección de Datos puede remitir la reclamación a:

- El delegado que haya seleccionado al responsable o encargado del tratamiento.

- El organismo de supervisión establecido para la aplicación de los códigos de conducta.

- El responsable o encargado del tratamiento, cuando no haya delegado ni esté adherido a mecanismos de resolución extrajudicial de conflictos. En este caso, el plazo de respuesta a la reclamación es de un mes.

Se debe notificar al reclamante la decisión sobre la admisión o inadmisión a trámite de la reclamación presentada en un plazo de tres meses.

2.11.3 Alcance territorial

Antes del resto de tareas, la Agencia Española de Protección de Datos debe examinar su competencia y determinar el alcance territorial del procedimiento. Esto no se aplica a los procedimientos en los que la Agencia Española de Protección de Datos sea la autoridad de control principal del tratamiento y alguna autoridad de control de otro Estado miembro de la Unión Europea le haya comunicado una reclamación formulada ante esta.

Cuando tras el análisis, la Agencia Española de Protección de Datos determine que no es ella misma la autoridad de control principal para la gestión del procedimiento, tiene que remitir la reclamación a la autoridad de control principal competente y notificar esta remisión al reclamante.

2.11.4 Actuaciones previas de investigación

A las actuaciones previas de investigación se les aplica lo dispuesto desde el apartado 8.6 al 8.9, sobre las potestades de investigación y los planes de auditoría preventiva, del Anexo D este documento.

La duración máxima de estas actuaciones es de 12 meses (desde el acuerdo de admisión a trámite o del acuerdo en el que se decide su iniciación) y su objetivo es determinar los hechos y circunstancias que prueben la tramitación del procedimiento.

2.11.5 Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora

Tras finalizar las actuaciones previas de investigación, la Presidencia de la Agencia de Protección de Datos puede iniciar el procedimiento para emplear la potestad sancionadora cuando corresponda. En este procedimiento se deben identificar los hechos y la persona o entidad que hubiera podido cometer una infracción, así como dicha infracción y su posible sanción.

Si en el procedimiento de cooperación entre las autoridades de control la Agencia Española de Protección de datos toma el papel de autoridad de control principal, el inicio del procedimiento para el ejercicio de la potestad sancionadora deberá cumplir con lo dispuesto en el artículo 60 del Reglamento (UE) 2016/679 sobre la Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.

2.11.6 Medidas provisionales y garantía de los derechos

Durante el procedimiento de actuaciones previas de investigación o al inicio del procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de datos puede tomar medidas urgentes para garantizar el derecho de protección de datos.

Si la Agencia Española de Protección de Datos cree que un tratamiento está provocando un grave daño al derecho de protección de datos personales, puede ordenar el bloqueo de los datos y el cese del tratamiento. Si no cumplen estas órdenes, la Agencia Española de protección de datos puede iniciar su inmovilización.

Además, si la Agencia Española de Protección de Datos recibe una reclamación de un afectado al que no le han atendido su solicitud para el ejercicio de sus derechos sobre el tratamiento en el plazo correspondiente, tras reunirse con el responsable puede establecer la obligación de atender al derecho solicitado por el reclamante y el resto de trámites que conlleve la reclamación.

2.12 Régimen sancionador

Tanto los responsables como los encargados de los tratamientos estaban sujetos al régimen sancionador de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, y ahora pasan a estar sujetos al régimen sancionador de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Además, con la entrada en vigor de la LOPDGDD, también están sujetos al régimen sancionador los representantes de los encargados o responsables de los tratamientos externos a la Unión Europea, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta.

La información relativa a sanciones y prescripciones se encuentra en el Anexo B y en cuanto a las infracciones, se identifican y clasifican en el siguiente subapartado.

2.12.1 Infracciones

Se considera infracción a cualquier acto o conducta contraria al Reglamento (UE) 2016/679 o a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Las infracciones se dividen en tres tipos, según la gravedad de estas, que se describen en la Tabla 3.

Tabla 3. Tipos de infracciones. Fuente: LOPDGDD.

Infracciones muy graves	Incumplir los principios y garantías del tratamiento dispuestos en el artículo 5 del Reglamento (UE) 2016/679.
	Realizar un tratamiento ilícito, es decir, que no cumpla ninguna de las condiciones de licitud dispuestas en el artículo 6 del Reglamento (UE) 2016/679.
	Incumplir las condiciones para el consentimiento del interesado dispuestas en el artículo 7 del Reglamento (UE) 2016/679.
	Usar los datos personales para una finalidad incompatible con la finalidad para la cual fueron recogidos, sin que lo consienta una base legal o el afectado.
	Tratar datos personales de carácter especial sin estar bajo alguna de las circunstancias dispuestas en el artículo 9 del Reglamento (UE) 2016/679 y en el artículo 9 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Tratar datos personales de condenas e infracciones penales o medidas de seguridad conexas en casos distintos a los mencionados en el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Tratar datos personales referentes a infracciones y sanciones administrativas en casos distintos a los dispuestos en el artículo 27 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Incumplir el deber de informar al afectado sobre el tratamiento de sus datos personales, descrito en los artículos 13 y 14 del Reglamento (UE) 2016/679 y en el artículo 12 de la Ley Orgánica de Protección de Datos Personales y

	Garantía de los Derechos Digitales de 2018.
	Quebrantar el deber de confidencialidad dispuesto en el artículo 5 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Cobrar al afectado por informarle sobre el tratamiento de sus datos o atender a las solicitudes para el ejercicio de sus derechos sobre el tratamiento cuando estas solicitudes no sean infundadas ni excesivas.
	Reiteradamente no atender o dificultar el ejercicio de los derechos del afectado sobre el tratamiento.
	Realizar una transferencia internacional de datos personales a una organización internacional o a alguien situado en un tercer país, sin que se cumpla lo dispuesto en los artículos 44 a 49 del Reglamento (UE) 2016/679.
	Incumplir las decisiones tomadas por una autoridad de protección de datos competente en el desempeño de los poderes que se le conceden en el artículo 58.2 del Reglamento (UE) 2016/679.
	Incumplir la obligación de bloqueo de datos en los casos mencionados en el artículo 32 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Impedir el ejercicio de los poderes de investigación de una autoridad de protección de datos al no facilitarle el acceso al contenido que requiera.
	Dificultar o impedir que una autoridad de protección de datos competente ejerza su función inspectora.
	Revertir a propósito un proceso de anonimización para volver a identificar a los afectados.
Infracciones graves	Tratar datos personales de un menor de edad sin su consentimiento, cuando este tenga entre 16 y 18 años, o el consentimiento del titular de su patria potestad o tutela.
	No demostrar que se ha trabajado en verificar la validez del consentimiento de un menor de edad o del titular de su patria potestad o tutela.
	Reiteradamente no atender o dificultar el ejercicio de los derechos de un afectado que haya facilitado datos personales que lo puedan identificar, para un tratamiento que no requiera la identificación del afectado.
	No llevar a cabo las medidas para la protección de datos desde el diseño ni ofrecer las garantías necesarias para el tratamiento, dispuestas en el artículo 25 del Reglamento (UE) 2016/679.
	No adoptar las medidas necesarias para garantizar un nivel de seguridad apropiado para el riesgo del tratamiento.
	Incumplir las medidas implantadas en materia de seguridad del tratamiento dispuestas en el artículo 32.1 del Reglamento (UE) 2016/679.
	Quebrantar el deber de elegir un representante de un responsable o encargado del tratamiento no establecido en la Unión Europea, descrito en el artículo 27 del Reglamento (UE) 2016/679.
	El representante, de un responsable o encargado del tratamiento no establecido en la Unión Europea, no atienda las solicitudes del afectado o de la autoridad de protección de datos competente.
	El responsable contrata a un encargado que no presenta las garantías necesarias para tomar las medidas apropiadas según lo dispuesto en el Capítulo IV del Reglamento (UE) 2016/679.
	Hacer que un tercero lleve a cabo el tratamiento de datos sin formalizar un contrato u otro acto jurídico que contenga lo establecido en el artículo 28.3 del Reglamento (UE) 2016/679.
	Un encargado del tratamiento contrata a otros encargados sin la autorización del responsable.
	Un encargado infringe la normativa de protección de datos personales al

	determinar los fines y medios del tratamiento.
	No llevar un registro, de todas las actividades de tratamiento realizadas, con el contenido establecido en el artículo 30 del Reglamento (UE) 2016/679.
	No proporcionar el registro de actividades de tratamiento a la autoridad de protección de datos que lo solicite.
	No cooperar con las autoridades de control en el ejercicio de sus funciones para asuntos no contemplados en la sección de infracciones muy graves de esta misma tabla.
	Realizar un tratamiento de datos sin haber valorado previamente los elementos dispuestos en el artículo 28 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	El encargado del tratamiento incumple su obligación de notificar al responsable del tratamiento cualquier violación de seguridad de la que sea consciente.
	Incumplir la obligación de notificar una violación de seguridad de los datos personales a la autoridad de protección de datos o al afectado conforme a lo dispuesto en los artículos 33 y 34 del Reglamento (UE) 2016/679.
	Realizar un tratamiento de datos sin llevar a cabo, cuando sea exigible, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales.
	Tratar datos personales sin antes consultárselo a la autoridad de protección de datos cuando una evaluación de impacto determine que este tratamiento conlleva un gran riesgo si el responsable no toma ciertas medidas o cuando una ley lo exija.
	Incumplir la obligación de designar un delegado en los casos mencionados en el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Dificultar al delegado de protección de datos el ejercicio de sus funciones.
	Usar un sello o certificación, en materia de protección de datos, no válido ya sea porque la vigencia del mismo haya expirado o porque lo hubiese otorgado una entidad de certificación no acreditada.
	Obtener la acreditación como organismo de certificación habiendo presentado información inexacta sobre el cumplimiento de las condiciones demandadas por el artículo 43 del Reglamento (UE) 2016/679.
	Ejercer funciones propias de un organismo de certificación sin tener la acreditación de institución de certificación dispuesta en el artículo 39 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Un organismo de certificación incumple alguno de los principios o deberes a los que está sujeto según lo dispuesto en los artículos 42 y 43 del Reglamento (UE) 2016/679.
	Ejercer funciones propias de un organismo de supervisión de códigos de conducta, previstas en el artículo 42 del Reglamento (UE) 2016/679, sin estar acreditado por la autoridad de protección de datos competente.
	Un organismo acreditado de supervisión de un código de conducta no tome las medidas adecuadas cuando se haya producido una infracción del código.
Infracciones leves	No proporcionar al afectado toda la información que exigen los artículos 13 y 14 del Reglamento (UE) 2016/679.
	Exigir al afectado una cuantía económica superior a los costes afrontados por facilitarle la información dispuesta en los artículos 13 y 14 del Reglamento (UE) o por atender sus solicitudes de ejercicio de sus derechos sobre el tratamiento, cuando las solicitudes sean infundadas o excesivas.
	No atender las solicitudes de ejercicio de los derechos del afectado sobre el tratamiento, a menos que fuese reiteradamente (ya que esto se consideraría

	infracción muy grave).
	No atender las solicitudes de ejercicio de los derechos de un afectado que haya facilitado datos personales que lo puedan identificar para un tratamiento que no requiera la identificación del afectado, a menos que fuese reiteradamente (ya que esto se consideraría infracción grave).
	Incumplir la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento prevista en el artículo 19 del Reglamento (UE) 2016/679.
	No informar al afectado sobre los destinatarios a los cuales se hayan comunicado datos personales modificados, suprimidos o respecto de los que se haya limitado el tratamiento, cuando el afectado lo haya solicitado.
	No suprimir los datos de un fallecido cuando lo haya solicitado alguien capacitado según lo dispuesto en el artículo 3 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.
	Los corresponsables del tratamiento no formalizan un acuerdo que contenga sus obligaciones, funciones y responsabilidades sobre el tratamiento y sus relaciones con los afectados, o si dicho acuerdo tiene contenido inexacto.
	No proporcionar a los afectados los aspectos esenciales del acuerdo entre los corresponsables del tratamiento.
	El encargado del tratamiento no informa al responsable del tratamiento sobre una posible infracción del Reglamento (UE) 2016/679 o de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, debida a una instrucción suya.
	El encargado incumple las instrucciones del responsable del tratamiento o el contrato o acto jurídico que regula el tratamiento, menos cuando sea para evitar una infracción de la normativa de protección de datos personales o cuando sea obligado por esta normativa.
	Tener un registro de actividades de tratamiento incompleto, es decir, que no incluya todo lo exigido en el artículo 30 del Reglamento (UE) 2016/679.
	No realizar correctamente la notificación a la autoridad de protección de datos competente descrita en el artículo 33 del Reglamento (UE) 2016/679.
	No documentar las violaciones de seguridad de los datos personales.
	No comunicar al afectado las violaciones de la seguridad de los datos personales que puedan implicar un alto riesgo para sus derechos y libertades, exceptuando el caso en que la autoridad de protección de datos hubiera exigido al responsable del tratamiento realizar esta notificación.
	Proporcionar información inexacta, a la Autoridad de protección de datos, a la hora de realizar la consulta previa descrita en el artículo 36 del Reglamento (UE) 2016/679.
	No publicar los datos de contacto del delegado de protección de datos, cuando lo haya, o no comunicarlos a la autoridad de protección de datos.
	Un organismo de certificación incumple la obligación de informar, a la autoridad de protección de datos competente, sobre la expedición, renovación o retirada de una certificación.
	Un organismo acreditado de supervisión de un código de conducta incumple la obligación de informar, a las autoridades de protección de datos, sobre las medidas a realizar en caso de infracción del código

3. Lista de tareas pendientes

Para realizar la lista de tareas pendientes se ha decidido utilizar software de hojas de cálculo, en este caso Microsoft Excel. El motivo de tomar esta decisión es la posibilidad de obtener más conocimiento puesto que no se ha profundizado en el aprendizaje de esta aplicación en la carrera a pesar de su gran importancia en el sector. La otra opción era programar una aplicación, sin embargo, como sí que se ha profundizado tanto en diseño de interfaces como en programación, era menos provechoso.

En cuanto al proceso de creación de la lista, se han de seguir unos pasos, puesto que no es simplemente rellenar las casillas. Primero, sabiendo que vamos a necesitar casillas hay que activar la opción para poder insertarlas, ya que por defecto en Excel no está activada. Para ello, hay que seleccionar la opción "Personalizar la cinta de opciones…" que aparece al clicar con el botón derecho del ratón encima de la cinta, tal y como se muestra en la Imagen 1.

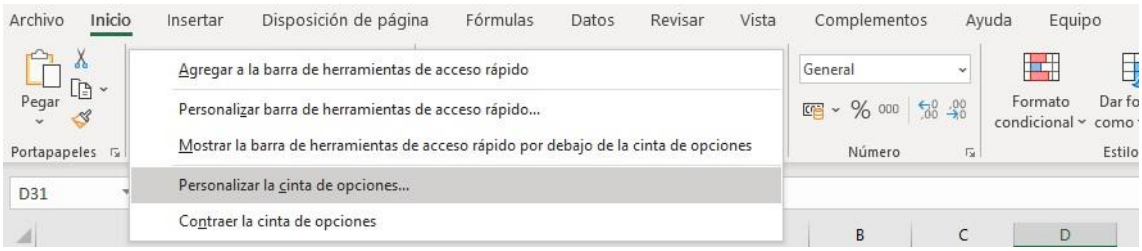

Imagen 1. Personalizar cinta de opciones. Fuente: elaboración propia.

Tras seleccionar esta opción, aparecerá una ventana a través de la cual es posible personalizar las pestañas que se visualizan en la interfaz del programa. La pestaña necesaria para poder insertar casillas es la de "Programador", por lo tanto, hay que marcarla tal y como figura en la Imagen 2. Tras marcar esa casilla hay que clicar "Aceptar" para guardar los cambios.

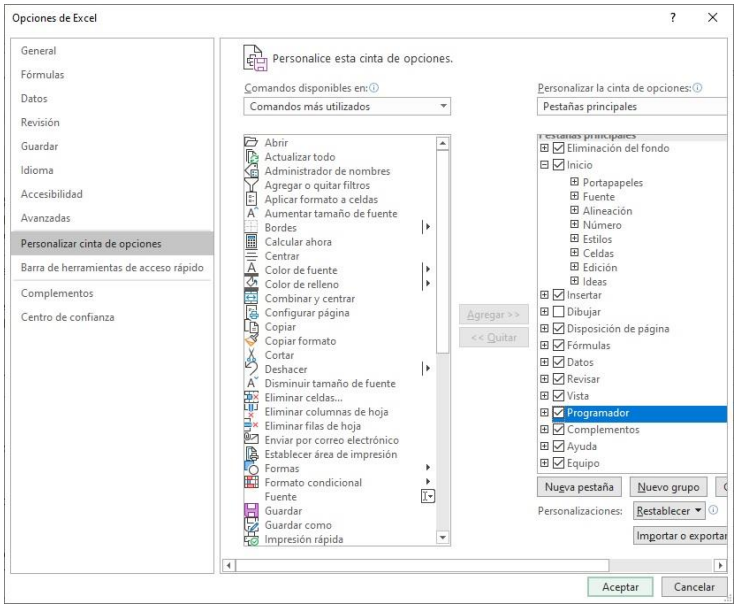

Imagen 2. Activar pestaña programador. Fuente: elaboración propia.

El siguiente paso es añadir tareas, que se han ido mencionando durante todo el documento, a una de las columnas de la hoja de cálculo, y una vez completado el listado hay que insertar casillas que se puedan marcar y asignarlas a las celdas correspondientes. Para agilizar el proceso hay que seguir los pasos que se describen a continuación.

Primero se inserta una única casilla, para ello hay que seleccionar la "Casilla (control de formulario)" a través de la opción insertar de la pestaña "Programador" como se muestra en la Imagen 3.

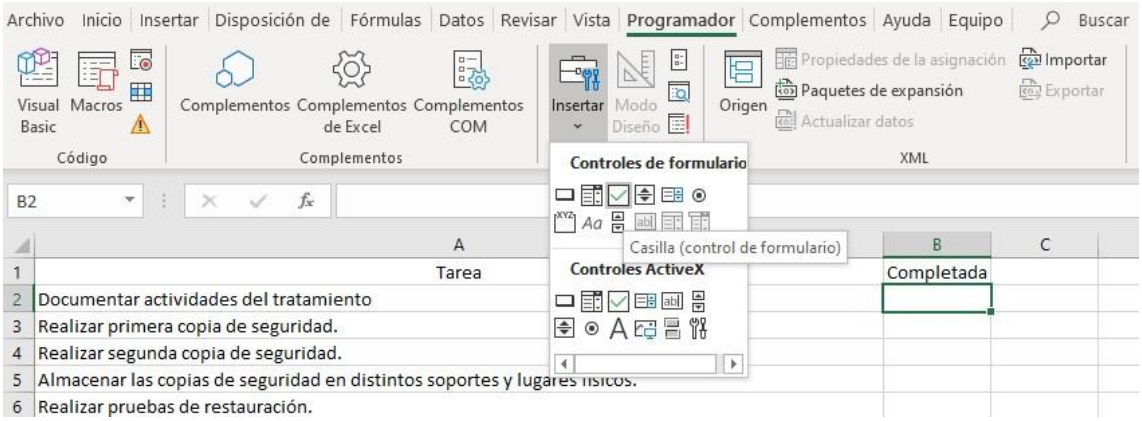

Imagen 3. Insertar casilla. Fuente: elaboración propia.

Después, hay que clicar la celda correspondiente (que está justo al lado de la primera tarea de la lista). De esta manera se insertará en la celda, pero no estará bien posicionada, para moverla simplemente hay que arrastrarla con el ratón y colocarla en la zona deseada. Tras esto es necesario borrar el texto que viene por defecto clicando con el botón derecho en la casilla y seleccionando "Editar texto".

Una vez la casilla esté insertada en la celda correspondiente y bien posicionada, es el momento de agilizar el proceso. Teniendo la celda de la casilla seleccionada, hay que clicar en el borde inferior derecho de la celda y arrastrar verticalmente hasta la fila correspondiente a la última tarea de la lista.

La idea es que las tareas que tengan la casilla marcada aparezcan tachadas en la lista, por lo tanto, primero es necesario enlazar la casilla a otra celda de manera que genere un valor (verdadero o falso) en función de si está marcada o no. Este proceso debe de realizarse individualmente en todas las tareas y consiste en hacer clic derecho en la casilla, seleccionar "Formato de control…" y a la derecha de "Vincular con la celda" seleccionar la casilla vacía en la que queremos que se genere el valor booleano utilizando la fecha que señala arriba.

Cuando ya esté completa toda columna de booleanos, se procede a aplicar un formato condicional a la lista de las tareas. Para ello hay que seleccionar todas las tareas y clicar en "Nueva regla…" a través de la opción "Formato condicional" de la pestaña "Inicio". Tras esto debe aparecer una ventana para la creación de la regla condicional y para lograr el efecto deseado hay que seleccionar como tipo de regla "Utilice una fórmula que determine las celdas para aplicar formato", después introducir la formula "=$C2=VERDADERO" (siendo C2 la celda donde se encuentra el valor booleano asociado a la primera casilla) tal y como indica la Imagen 4.

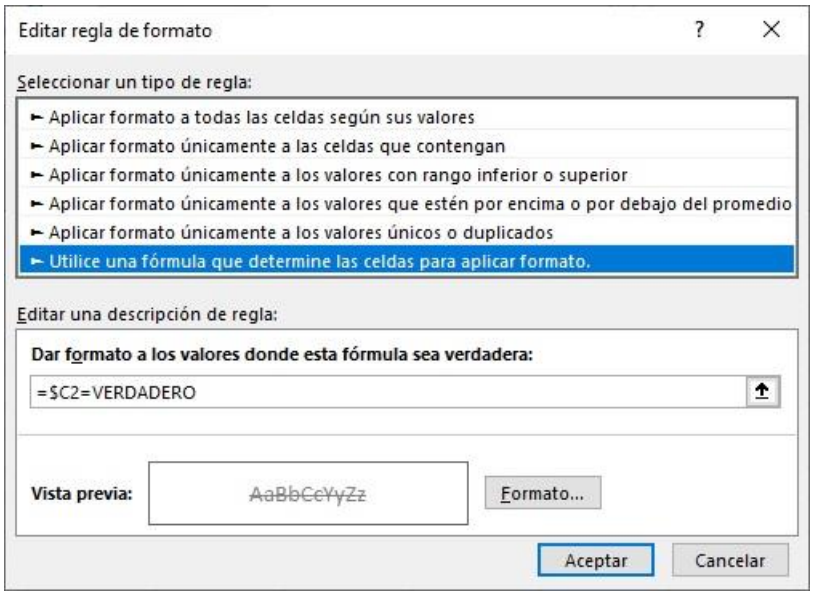

Imagen 4. Nueva regla de formato condicional. Fuente: elaboración propia.

Tras esto, clicar en “Formato…” para poder seleccionar el formato deseado, en este caso color gris y efecto tachado. Por último, hay que aceptar tanto la ventana de “Formato de celdas” como la de “Editar regla de formato” para que se apliquen los cambios.

Por último, hay que ocultar la columna de los valores booleanos, ya que no son datos que deban estar visibles porque solo sirven para darle funcionalidad a las casillas. Esto se consigue clicando con el botón derecho del ratón en la columna y seleccionando “Ocultar”.

4. Conclusiones

Mientras desarrollaba el trabajo me encontré ante un gran problema. Resulta que la ley de protección de datos salió en diciembre y en ese entonces yo ya había leído y desarrollado parte del trabajo con los documentos urgentes de adaptación al reglamento europeo. Por lo tanto, tuve que eliminar todo lo que había hecho e intentar olvidarlo para evitar redactar información desactualizada.

Durante la carrera he utilizado programas de hojas de cálculo, pero siempre ha sido de un modo básico, sin embargo, al realizar este trabajo he aprendido cosas más complejas al hacer uso de las opciones de programador como, por ejemplo, la creación de “checkboxes” y su asignación a las casillas de la hoja de cálculo.

También, he podido conocer en profundidad la normativa de protección de datos actual, una materia muy importante para las empresas debido a la gran cantidad de datos que se tratan hoy en día.

Si tengo que valorar el trabajo, he de decir que estoy contento con el resultado, puesto que como se puede demostrar por lo descrito en este apartado de conclusiones puedo decir que se han alcanzado los objetivos descritos al inicio del desarrollo del trabajo.

5. Anexo A: Garantía de los derechos digitales

Uno de los grandes añadidos de la LOPDGDD es la garantía de los derechos digitales, debido a la gran importancia que ha tomado Internet durante los últimos años. El tema de los derechos digitales se trata en 18 artículos, los cuales no están presentes en el Reglamento (UE) 2016/679 y su relevancia es tal que se ha modificado el nombre de la LOPD, pasándose a llamar Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

5.1 Derecho a la neutralidad de internet

Por un lado, los usuarios tienen derecho a que todos los datos que circulen por internet se traten de la misma manera, sin que se les cobre una tarifa según el contenido al que accedan y, por otro lado, los proveedores de servicios de Internet deben ofertar sus servicios sin discriminar a nadie por motivos económicos o técnicos.

5.2 Derecho de acceso universal a internet

Todos tienen garantizado el acceso universal, asequible y de calidad a Internet independientemente de su condición social, personal, geográfica o económica. El acceso a Internet pretende superar tanto la brecha de género como la brecha generacional, toma en consideración la realidad específica de los entornos rurales y garantiza condiciones de igualdad para las personas que tengan necesidades especiales.

5.3 Derecho a la seguridad digital

Los usuarios tienen derecho a la seguridad de las comunicaciones de las que sean partícipes y los ISP son los encargados de informarles sobre estos derechos.

5.4 Derecho a la educación digital

El profesorado debe recibir las competencias digitales y la formación necesaria para adecuarse a un sistema educativo que garantice al alumnado el aprendizaje de un uso seguro y respetuoso de los medios digitales.

Las Administraciones Públicas deben incluir materias sobre la garantía de los derechos digitales y la protección de datos a los temarios de las pruebas de acceso.

Los planes de estudio de títulos universitarios deben garantizar la formación en la garantía de los derechos fundamentales de Internet y en el uso y seguridad de los medios digitales.

5.5 Protección de los menores en Internet

Para garantizar la protección de los menores en Internet es necesario que los padres, las madres o los representantes legales, los centros educativos y el Ministerio Fiscal realicen las labores que les corresponden respecto a este tema.

La labor de los padres, las madres o los representantes legales es intentar que los menores de edad hagan un uso equilibrado y responsable de los dispositivos y servicios digitales para garantizar su desarrollo personal y proteger su dignidad y sus derechos fundamentales.

El Ministerio Fiscal hará que se tomen las medidas cautelares y de protección dispuestas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, cuando el uso o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes puedan suponer una intromisión ilegítima en sus derechos fundamentales.

Los centros educativos deben garantizar la protección del interés superior del menor y sus derechos fundamentales cuando publiquen o difundan sus datos personales a través de servicios de la sociedad de la información. En caso de que esta publicación o difusión se lleve a cabo en redes sociales o servicios equivalentes, deben contar con el consentimiento del menor o de sus representantes legales cuando el menor no esté capacitado para darlo.

5.6 Derecho de rectificación en Internet

Los responsables de redes sociales y servicios similares deben adoptar protocolos para hacer posible el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que vulneren el derecho al honor, la intimidad personal y familiar en Internet y el derecho a obtener o proporcionar libremente información verídica.

En el caso de que los medios de comunicación digitales tengan que atender una solicitud de rectificación, deben publicar un aviso aclaratorio, en un lugar visible junto a la información original, que deje claro que la noticia original no refleja la situación actual del individuo.

5.7 Derecho a la actualización de informaciones en medios de comunicación digitales

Todos tienen el derecho de solicitar a los medios de comunicación digitales que se incluya un aviso de actualización visible junto a las noticias que no reflejen su situación actual. Estos medios llevarán a cabo esta inclusión cuando la información original se refiera a actuaciones policiales o judiciales que se hayan visto afectadas a favor del interesado como consecuencia de decisiones judiciales posteriores.

5.8 Derecho a la intimidad en el ámbito laboral

Los empleados tienen derecho a la protección de su intimidad en el uso de dispositivos digitales puestos a disposición por su empleador, siguiendo las normas de uso, fijadas por el empleador, que le hayan sido comunicadas.

El empleador puede acceder al contenido derivado del uso de medios digitales facilitados a los trabajadores únicamente para controlar el cumplimiento de las obligaciones del empleado y de garantizar la integridad de estos dispositivos.

Cuando se utilicen dispositivos de vigilancia, sistemas de geolocalización o dispositivos de grabación de sonidos en el ámbito laboral, los empleadores tendrán que informar claramente sobre esto a los empleados. En el caso de que se haya captado la comisión de un acto ilícito por parte de un empleado, el deber de información se considerará cumplido si por lo menos existe un dispositivo informativo en un lugar suficientemente visible.

Tanto el tratamiento de datos obtenidos mediante sistemas de geolocalización, como el tratamiento de las imágenes obtenidas por medio de los dispositivos de vigilancia lo pueden llevar a cabo los empleadores para el ejercicio de las funciones de control de los empleados.

En cuanto a los sistemas de grabación de sonido, solo se permitirá su uso cuando sean relevantes los riesgos para la seguridad de las instalaciones, bienes y personas.

La instalación de los dispositivos de videovigilancia y grabación de sonido queda terminantemente prohibida en los lugares de descanso de los empleados.

5.9 Derecho a la desconexión digital en el ámbito laboral

Los empleados tienen derecho a la desconexión digital para asegurar que se respete su intimidad personal y familiar, su tiempo de descanso, sus permisos y sus vacaciones.

Tras reunirse con los representantes de los trabajadores, el empleador realizará una política interna dirigida a trabajadores para definir la forma en la que se ejercerá este derecho.

5.10 Derechos digitales en la negociación colectiva

Es posible, mediante convenios colectivos, añadir garantías adicionales de las derechos y libertades relacionados con el tratamiento de datos personales de los empleados y la protección de derechos digitales en el ámbito laboral.

5.11 Derecho al olvido

Todos tienen derecho a que se suprima la información (existente sobre el interesado) inexacta, inadecuada o que hubiera devenido como tal al cabo del tiempo, tanto en búsquedas de internet como en redes sociales y servicios equivalentes.

Cuando se trata de búsquedas en Internet, los motores de búsqueda deben eliminar, cuando proceda, determinados enlaces de la lista de resultados obtenida tras una búsqueda del nombre del interesado. Esto no impide que se pueda encontrar esos enlaces a través de la búsqueda de otro término.

Y en el caso de las redes sociales y servicios equivalentes se deben eliminar, cuando proceda, las publicaciones de datos personales del interesado facilitados por terceros, exceptuando los datos facilitados por personas físicas en el ejercicio de actividades personales o domésticas. El interesado también tiene derecho a solicitar que se supriman los datos facilitados por terceros durante su minoría de edad y los datos que haya facilitado él mismo, independientemente de si era menor o no.

5.12 Derecho de portabilidad en servicios de redes sociales y servicios equivalentes

Los usuarios tienen derecho a recibir y transmitir el contenido que hayan facilitado a los prestadores de servicios de redes sociales o equivalentes y, cuando sea técnicamente posible, también tienen derecho a que los prestadores transmitan el contenido directamente a otro prestador elegido por el interesado.

El contenido proporcionado por el interesado no pueden difundirlo los prestadores, pero si conservarlo para cumplir obligaciones legales.

5.13 Derecho al testamento digital

Tanto para el acceso al contenido del fallecido que gestionen los prestadores de servicios de la sociedad de la información, como para la toma de decisiones sobre el uso, destino o supresión de este contenido y de los perfiles personales del fallecido en redes sociales o servicios similares, se aplica lo previsto en el apartado “2.1 Datos de personas fallecidas” de este documento.

5.14 Políticas de impulso de los derechos digitales

Para favorecer los derechos digitales, el Gobierno confecciona un Plan de Acceso a Internet y un Plan de Actuación.

El Plan de Acceso a Internet tiene como objetivo superar las brechas digitales, promover espacios de conexión de acceso público y favorecer medidas educativas que promuevan la formación digital.

Y el Plan de Actuación tiene como objetivo garantizar el desarrollo de la personalidad de los menores de edad y proteger su dignidad y sus derechos fundamentales, mediante la promoción de acciones de formación, difusión y concienciación que logren que los menores hagan un uso equilibrado de los servicios digitales.

6. Anexo B: Prescripción y sanciones

6.1 Sanciones y medidas correctivas

La cuantía de las multas administrativas no depende únicamente de la infracción que se haya cometido sino también de muchos otros factores, lo que implica que el cálculo de la sanción económica se deba realizar para cada caso individual. Estos factores, descritos en el artículo 83.2 del Reglamento (UE) 2016/679 y en el artículo 76.2 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, son los siguientes:

- La naturaleza, gravedad y duración de la infracción.

- La intencionalidad o negligencia en la infracción.

- Las medidas llevadas a cabo por el responsable o encargado del tratamiento para mitigar los daños y perjuicios sufridos por los interesados.

- El grado de responsabilidad del responsable o encargado del tratamiento.

- Las infracciones previas cometidas por el responsable o encargado del tratamiento.

- El grado de cooperación con la autoridad de control para corregir la infracción y paliar las posibles consecuencias de la infracción.

- Las categorías de los datos personales afectados por la infracción.

- La existencia de la notificación a la autoridad de control, por parte del responsable o encargado del tratamiento, sobre la infracción cometida.

- El cumplimiento de las medidas exigidas al responsable o encargado del tratamiento, por parte de una autoridad de control.

- La conformidad con los códigos de conducta o los mecanismos de certificación de la normativa de protección de datos personales.

- El carácter continuado de la infracción.

- La existencia de una conducta del afectado que pueda incitar a realizar la infracción.

- Los beneficios obtenidos por haber realizado la infracción.

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

- Si la entidad que cometió la infracción ha sido absorbida por otra.

- La afectación a los derechos de los menores.

- Contar con un delegado de protección de datos, cuando no sea necesario.

- El sometimiento voluntario del responsable o encargado del tratamiento a mecanismos de resolución alternativa de conflictos, cuando tengan polémica con el interesado.

La Ley Orgánica de Protección de Datos de Carácter Personal de 1999 ya contemplaba alguno de los factores mencionados para graduar la cuantía de las sanciones, como por ejemplo el grado de intencionalidad, pero con la LOPDGDD se contemplan muchos más aspectos.

A pesar de que la cuantía de las sanciones se calcula según cada caso tomando en consideración una serie de factores, hay unos límites establecidos que no pueden superar. Estos límites han aumentado considerablemente con el cambio de la normativa de protección de datos, puesto que en la LOPD de 1999 la cuantía de las sanciones leves estaba entre 900 y 40.000 euros, la de las graves entre 40.001 y 300.000 euros y la de las muy graves entre 300.001 y 600.000 euros, sin embargo, en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 las multas pueden llegar a los 10 millones de euros (o al 2% del volumen de negocio total anual global de la empresa, si es superior a los 10 millones) cuando se incumplan las obligaciones de los organismos de certificación, de la autoridad de control o de los encargados y responsables del tratamiento, y a los 20 millones de euros (o al 4% del volumen de negocio total anual global de la empresa, si es superior a los 20 millones) cuando se infrinjan los principios básicos para el tratamiento o los derechos de los interesados.

6.2 Prescripción

Tanto las infracciones como las sanciones caducan al pasar una cantidad de tiempo determinada. Esta cantidad de tiempo depende de la gravedad, en caso de las infracciones, y de la cuantía económica, en caso de las sanciones.

Al igual que en la LOPD de 1999, las infracciones muy graves prescriben en tres años, las graves en dos y las leves en uno.

Hay dos motivos por los cuales se puede interrumpir la prescripción de una infracción. El primero es la iniciación del procedimiento sancionador con conocimiento del interesado, reiniciándose el plazo de prescripción cuando el expediente sancionador hubiese estado paralizado por más de 6 meses por causas no imputables al presunto culpable; y el segundo es el conocimiento formal del interesado del proyecto de acuerdo de inicio cuando se realice una cooperación entre autoridades de control en la cual la Agencia Española de Protección de Datos sea la autoridad de control principal.

Las sanciones prescriben en tres años cuando su importe es superior a 300.000 euros, en dos años cuando su importe está comprendido entre 40.001 y 300.000 euros y en un año cuando su importe es menor o igual a 40.000 euros.

El único motivo por el cual se puede interrumpir la prescripción de las sanciones es la iniciación del procedimiento de ejecución, con conocimiento del afectado, reiniciándose el plazo de prescripción cuando se hubiese paralizado por más de 6 meses por causas no imputables al infractor.

7. Anexo C: Cambios en otras leyes

Además de los cambios respecto a la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, la LOPDGDD también conlleva cambios en otras leyes. La modificación de estas leyes se describe en las disposiciones finales de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y son las que se tratan en este apartado.

7.1 Ley Orgánica del Régimen Electoral General

Por la disposición final tercera de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. Esta modificación consta de lo siguiente:

- La adición de una frase al apartado 3 del artículo 39 sobre la rectificación del censo en período electoral. Este añadido permite que, si lo solicitan, los electores puedan evitar recibir propaganda electoral a su domicilio y queda redactado de la siguiente manera:

> *También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral.*

- La adición del artículo 58 bis sobre el uso de medios tecnológicos y datos personales en actividades electorales, especifica que la propaganda electoral enviada por medios digitales no es considerada comunicación comercial y que para llevar a cabo actividades políticas en periodo electoral se puede hacer uso de datos personales que estén públicos en algún sitio web. Este artículo queda redactado tal que así:

> *Artículo 58 bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.*
>
> 1. *La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan las garantías adecuadas.*
> 2. *Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.*
> 3. *El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.*
> 4. *Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.*
> 5. *Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.*

7.2 Ley Orgánica del Poder Judicial

Por la disposición final cuarta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Las modificaciones llevadas a cabo en esta ley se centran en exigir el conocimiento sobre determinadas solicitudes de autorización que se tratan en los artículos 58, 66, 74 y 90 de esta ley y son las siguientes:

- Al artículo 58, sobre la Sala de lo Contencioso-administrativo del Tribunal Supremo, se le añade un tercer apartado cuyo contenido es el siguiente:

> *Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.*

- Al artículo 66, sobre la Sala de lo Contencioso-administrativo de la Audiencia Nacional, se le añade una letra f redactada de la siguiente manera:

> *f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.*

- Al artículo 74, sobre las Salas de lo Contencioso-Administrativo de los Tribunales Superiores de Justicia, se le realizan dos modificaciones. Por una parte, a su apartado 1 se le añade una letra k redactada de la siguiente forma:

> *k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.*

Y, por otra parte, se le añade un apartado 7 que dice lo siguiente:

> *7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.*

- Al artículo 90, sobre los Juzgados de lo Contencioso-administrativo, se le añade un apartado 7 redactado tal que así:

> *7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.*

7.3 Ley General de Sanidad

Por la disposición final quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 14/1986, de 25 de abril, General de Sanidad. Al Título VI de esta ley se le añade un Capítulo II, sobre el tratamiento de datos de la investigación en salud, que contiene el nuevo artículo 105 bis redactado tal que así:

> *Artículo 105 bis. El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.*

Y es que, entre otros aspectos, para llevar a cabo los tratamientos de datos en la investigación en salud debe suceder alguna de las siguientes circunstancias:

- El interesado, o cuando proceda, su representante legal haya otorgado su consentimiento para una finalidad concreta. Además, sin contar con más consentimientos también se podrá realizar el tratamiento de datos para finalidades similares o áreas de investigación relacionadas.

- Aun sin tener el consentimiento del interesado, cuando suponga algún peligro para la salud pública.

- Se usen datos personales seudonimizados para el tratamiento cuando se cumpla lo siguiente: que exista una separación entre los investigadores y los que llevan a cabo el proceso de seudonimización, que haya un compromiso de confidencialidad y de que no se realicen procesos para reidentificar a los afectados (salvo que exista un peligro para la salud pública) y que se tomen medidas de seguridad para evitar el acceso de terceros no autorizados y la reidentificación de los afectados.

7.4 Ley Reguladora de la Jurisdicción Contencioso-administrativa

Por la disposición final sexta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. Además de añadir el artículo 122 ter, se exige cierto conocimiento sobre las solicitudes de autorización al modificar los artículos 10, 11 y 12 de la siguiente manera:

- Al artículo 10, sobre las competencias de las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia, se le añade un apartado 7 redactado de la siguiente forma:

> *7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.*

- Al artículo 11, sobre los conocimientos de la Sala de lo Contencioso-administrativo de la Audiencia Nacional, se le añade un nuevo apartado 5 que queda descrito de la siguiente manera:

> *5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.*

- Al artículo 12, sobre los conocimientos de la Sala de lo Contencioso-administrativo del Tribunal Supremo, se le añade un apartado 4 redactado tal que así:

> *4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.*

- Por último, a esta ley se le añade el artículo 122 ter, la cual describe el proceso de autorización sobre transferencias internacionales de datos que se lleva a cabo desde la solicitud de la autoridad de protección de datos hasta la resolución de la misma por el Tribunal competente, cuyo contenido es el siguiente:

> *Artículo 122 ter. Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*
>
> 1. *El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos digitales se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.*
> 2. *Serán partes en el procedimiento, además de la autoridad de protección de datos,*

quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. *El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.*
4. *Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que de traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.*
5. *Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.*
6. *Transcurrido el periodo de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.*
7. *Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:*
   a) *Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.*
   b) *En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.*

   La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.
8. *El régimen de recursos será el previsto en esta ley.*

7.5 Ley de Enjuiciamiento Civil

Por la disposición final séptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Las modificaciones que sufre el artículo 15 bis de esta ley permiten que el artículo sea más completo, específico y que esté actualizado respecto a las leyes y artículos referenciados en el mismo. El artículo 15 bis queda de la siguiente forma:

Artículo 15 bis. Intervención en procesos de defensa de la competencia y de protección de datos.

1. *La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 Julio, de Defensa de la Competencia. Con la venia del correspondiente órgano*

jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.
La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. *La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.*
3. *Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.*

7.6 Ley Orgánica de Universidades

Por la disposición final octava de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades. La modificación del artículo 46, sobre los derechos y deberes de los estudiantes, de esta ley consiste en añadir a su segundo apartado una nueva letra l cuyo contenido es el siguiente:

l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

7.7 Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Por la disposición final novena de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Tras la modificación de esta ley, el apartado 3 del artículo 16, sobre los usos de la historia clínica, queda de la siguiente manera:

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga

a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

En este, se establece la necesidad de separación de datos, de manera que no se puedan identificar a los pacientes para determinados fines salvo que ocurran unas circunstancias específicas, como por ejemplo la posible existencia de una amenaza a la salud pública.

7.8 Ley Orgánica de Educación

Por la disposición final décima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación. Al sistema educativo español se le añade un nuevo objetivo mediante la adición de la nueva letra l al apartado 1 del artículo 2 cuyo contenido es el siguiente:

l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.

7.9 Ley de transparencia, acceso a la información pública y buen gobierno

Por la disposición final undécima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Las modificaciones llevadas a cabo en esta ley son las siguientes:

- La adición del artículo 6 bis, sobre la obligación de publicar el registro de actividades de determinados tratamientos, cuyo contenido es el siguiente:

> *Artículo 6 bis. Registro de actividades de tratamiento.*
> *Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.*

- La modificación del apartado 1 del artículo 15, sobre la protección de datos personales, la cual consiste en sustituir las referencias a la LOPD de 1999 por las categorías especiales de datos correspondientes a cada caso. Dicho apartado queda redactado de la siguiente manera:

> *1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.*
> *Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.*

7.10 Ley del Procedimiento Administrativo Común de las Administraciones Públicas

Por la disposición duodécima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Se modifica el artículo 28, sobre el derecho de los interesados a no aportar documentos al procedimiento administrativo en determinadas situaciones y el deber de las administraciones en materia de la obtención de estos documentos, en concreto sus apartados 2 y 3, que quedan redactados tal que así:

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.
Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.
Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.
Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

7.11 Texto refundido de la Ley del Estatuto de los Trabajadores

Por la disposición final decimotercera de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica el texto refundido de la Ley del Estatuto de los Trabajadores. Esta modificación consiste en la adición del artículo 20 bis, sobre el derecho a la intimidad de los trabajadores, redactado de la siguiente forma:

Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.
Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Esto hace referencia a los artículos 87, 88, 89 y 90 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018. En el presente documento, la información sobre estos derechos de la intimidad y desconexión digital en el ámbito laboral se encuentra en los apartados 8 y 9 del Anexo A.

7.12 Texto refundido de la Ley del Estatuto Básico del Empleado Público

Por la disposición final decimocuarta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales se modifica el texto refundido de la Ley del Estatuto Básico del Empleado Público. Esta modificación consiste en dotar a los empleados públicos de un nuevo derecho individual mediante la adición de la nueva letra j bis al artículo 14 que dice lo siguiente:

> *j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.*

Al igual que los trabajadores, los empleados públicos también obtienen el derecho a la intimidad y desconexión laboral en el ámbito laboral, así que a este apartado se le aplica lo dispuesto en el último párrafo del apartado “7.11 Texto refundido de la Ley del Estatuto de los Trabajadores” de este documento.

8. Anexo D: Agencia Española de Protección de Datos

8.1 Disposiciones generales y régimen jurídico y económico

La Agencia Española de Protección de Datos se relaciona con el Gobierno a través del Ministerio de Justicia, actúa como representante común de las autoridades de protección de datos de España en el Comité Europeo de Protección de Datos y colabora con el Consejo General del Poder Judicial para el desempeño de sus funciones sobre protección de datos en el ámbito de la Administración de Justicia.

Tras el cambio en la ley orgánica de protección de datos, la Agencia Española de Protección de Datos se rige por lo establecido en el Reglamento (UE) 2016/679, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y sus disposiciones de desarrollo. Además, también se regirá por lo dispuesto en el artículo 110.1 de la Ley 40/2015 de Régimen Jurídico del Sector Público, siempre y cuando no vaya en contra de lo citado en el artículo 63.2 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y sea compatible con su plena independencia.

En cuanto al régimen económico, sigue siendo la propia Agencia Española de Protección de Datos quien elabora y aprueba su presupuesto. El Gobierno, al igual que en la Ley Orgánica de Protección de Datos Personales de 1999, se encarga de integrar este presupuesto en los Presupuestos Generales del Estado.

Los encargados de autorizar las modificaciones en el presupuesto son:

- La Presidencia de la Agencia Española de Protección de Datos, cuando las modificaciones a realizar supongan, como máximo, el incremento de un tres por ciento de la cifra inicial del presupuesto, siempre que no se incrementen los créditos para gastos de personal.

- El Ministerio de Hacienda, cuando el incremento del presupuesto esté entre un 3 y un 5 por ciento de la cifra inicial del presupuesto.

- El Gobierno, en el resto de las situaciones.

Para cumplir con sus fines, la Agencia Española de Protección de Datos contará con los mismos bienes y medios económicos que le permitía la Ley de Protección de Datos de Carácter Personal de 1999, pero añadiendo los derivados del ejercicio de los poderes citados en el artículo 58 del Reglamento (UE) 2016/679. El resultado positivo de los ingresos obtenidos por la Agencia Española de Protección de Datos se reservará para poder garantizar su independencia.

Según lo establecido en la Ley General Presupuestaria de 2003 y sin perjuicio de los poderes concedidos al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos debe someterse al control de la Intervención General de la Administración del Estado.

Y en cuanto al régimen de personal, los trabajadores que están al servicio de la Agencia Española de Protección de Datos deben ser funcionarios o laborales que se rijan por lo dispuesto en el texto refundido de la Ley del Estatuto Básico del Empleado Público aprobado por real decreto en 2015, la normativa reguladora de funcionarios públicos y la normativa laboral que corresponda.

La Agencia Española de Protección de Datos también se encarga de elaborar y aprobar su relación de puestos de trabajo sin sobrepasar el límite del gasto de personal establecido en su presupuesto. En esta relación se incluyen los puestos de trabajo que solo pueden ser llevados a cabo por un funcionario público debido a la necesidad de ejercer potestades públicas y salvaguardar los intereses generales del Estado y de las Administraciones Públicas.

8.2 Funciones

La Agencia Española de Protección de Datos se encarga de desempeñar las funciones relacionadas con la protección de datos personales, esto incluye hacer que el público valore y comprenda los riesgos, normas, garantías y derechos que conlleva un tratamiento de datos, y muchas otras funciones que se describen a continuación.

La agencia asesora a otras instituciones y organismos sobre las medidas legislativas y administrativas referentes a la protección de los derechos y libertades de las personas físicas correspondientes al tratamiento de datos.

También se encarga de cooperar con otras autoridades de control y prestar asistencia mutua para garantizar la coherencia en la aplicación y ejecución del presente reglamento de protección de datos.

Basándose en la información recibida de una autoridad de control o autoridad pública, la Agencia Española de Protección de Datos lleva a cabo investigaciones acerca de la aplicación del vigente reglamento de protección de datos.

Otra de las funciones de la Agencia Española de Protección de datos es realizar un seguimiento de los cambios que puedan afectar a la protección de datos personales, especialmente el desarrollo de tecnologías de información y la comunicación y las prácticas comerciales.

La Agencia Española de Protección de Datos se encarga de adoptar cláusulas contractuales tipo siguiendo el mecanismo de coherencia establecido en el reglamento europeo, para regular y definir el tratamiento llevado a cabo por el encargado o para imponer obligaciones a un nuevo encargado. Además, adopta clausulas tipo de protección de datos que ofrecen las garantías adecuadas para que el encargado pueda transmitir datos personales a un tercer país u organización internacional.

Debido a que muchos tratamientos requieren una previa evaluación de impacto por tener operaciones que conllevan un alto riesgo para los derechos y libertades de las personas físicas, la Agencia Española de Protección de Datos debe elaborar y mantener un listado de este tipo de operaciones, de esta forma los responsables de cualquier tratamiento de datos personales pueden saber cuándo es obligatorio realizar dicha evaluación.

Otra de sus funciones es asesorar al responsable del tratamiento, y en su caso al encargado, sobre las operaciones que supongan un alto riesgo, para los derechos de los afectados, que el responsable todavía no haya identificado o mitigado.

Asimismo, se encarga tanto de animar a que se elaboren códigos de conducta, que contribuyen a que se aplique correctamente el reglamento de protección de datos, como de dictaminar y aprobar los códigos de conducta que cumplan con las garantías adecuadas.

También fomenta la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos para probar que se cumple la normativa de protección de datos, además, la Agencia Española de Protección de Datos se encarga de aprobar los criterios de certificación.

Cuando sea necesario, lleva a cabo revisiones periódicas de las certificaciones expedidas a un responsable o encargado de tratamiento, ya que estas certificaciones tienen una validez máxima de 3 años y pueden ser renovadas en el caso de que siga cumpliendo los requisitos adecuados.

Tanto los organismos de supervisión de los códigos de conducta como los organismos de certificación necesitan estar acreditados para llevar a cabo sus funciones, y es la Agencia Española de Protección de Datos la encargada de acreditarlos y de elaborar y publicar los criterios para llevar a cabo esta acreditación.

También aprueban normas corporativas vinculantes de acuerdo con el mecanismo de coherencia siempre que estas normas sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes a las empresas que realicen una actividad conjunta, otorguen a los interesados los derechos exigibles relativos al tratamiento de sus datos personales y por lo menos, especifiquen los siguientes elementos citados del artículo 47.2 del Reglamento (UE) 2016/679:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

La Agencia Española de protección de datos contribuye a las tareas del Comité Europeo de Protección de Datos.

Otra de las funciones que tiene la Agencia es llevar registros internos de las infracciones de la vigente normativa de protección de datos personales y de los poderes correctivos utilizados para sancionar estas infracciones.

Y no hay solamente funciones nuevas, sino que además se mantienen algunas funciones que tenía asignadas la Agencia Española de Protección de Datos en la anterior ley de protección de datos, solo que en algunos casos actualizándose a la situación actual.

Respecto a la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 se conserva la función de controlar que se aplique el reglamento de protección de datos vigente, que en este caso pasa a ser la presente Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y el Reglamento (UE) 2016/679.

También se sigue encargando de autorizar lo previsto en la Ley o en sus disposiciones reglamentarias, ahora tomando en especial consideración lo mencionado en el artículo 42 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y las cláusulas citadas en el artículo 46.3 del Reglamento (UE) 2016/679.

Además, continúan tratando las peticiones y reclamaciones del interesado o su representante, incluyendo la investigación del motivo de la reclamación e informar al reclamante sobre el curso y resultado de dicha investigación en un plazo razonable, especialmente si se consideran necesarias nuevas investigaciones o coordinarse con otra autoridad de control.

Al igual que en la antigua ley de 1999, deben proporcionar a los interesados toda la información referente al ejercicio de sus derechos en materia de protección de datos.

Siguen encargándose de fomentar que los responsables y encargados den importancia a sus obligaciones respecto al reglamento de protección de datos personales, de manera que adopten las medidas necesarias para su cumplimiento.

Otra de las funciones que conserva la Agencia es la de publicar resoluciones. Además de las dispuestas en su Estatuto, las resoluciones de su Presidencia son:

- Las que ponen fin a alguna reclamación.

- Las que imponen medidas cautelares.

- Las que tienen relación con los derechos del interesado respecto al tratamiento de datos, es decir, los derechos tratados en los artículos comprendidos entre el 15 y el 22 del Reglamento (UE) 2016/679.

- Las que archivan las actuaciones previas de investigación.

- Las que, tras haber dado un aviso previamente para que no persista una falta, sancionan a los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, el Banco de España, las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las fundaciones del sector público, las Universidades Públicas, los consorcios y los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

8.3 Poderes

Antiguamente, con la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, las potestades de la Agencia se limitaban a la inspección de ficheros y al ejercicio de la potestad sancionadora, sin embargo, con el cambio de normativa de protección de datos, la Agencia Española de Protección de Datos dispone de tres conjuntos de poderes: poderes de investigación, poderes correctivos y poderes de autorización y consultivos.

Los poderes de investigación son los siguientes:

- Exigir al responsable y al encargado, o al representante de alguno de ellos, que le proporcionen tanto la información requerida como el acceso todos los datos personales y a la información necesaria para realizar sus funciones.

- Obtener acceso a todos los locales del encargado y responsable del tratamiento, así como a los equipos y medios de tratamiento de datos.

- Realizar revisiones de los certificados de protección de datos para comprobar si siguen cumpliendo los requisitos que garanticen el cumplimiento de la normativa de protección de datos.

- Efectuar investigaciones a modo de auditorías de protección de datos.

- Notificar cualquier supuesta infracción de la normativa de protección de datos al encargado o responsable del tratamiento.

Los poderes correctivos son los indicados a continuación:

- Sancionar a los responsables o encargados del tratamiento con una advertencia, si hay posibilidad de que el tratamiento incumpla lo dispuesto en la normativa de protección de datos, o con apercibimiento si finalmente lo infringen.

- Imponer tanto multas administrativas por incumplimiento de la normativa de protección de datos, como limitaciones o prohibiciones de los tratamientos.

- Hacer que se retire una certificación sobre protección de datos ya emitida o evitar que se emita una certificación cuando no se cumplan los requisitos adecuados.

- Ordenar al responsable o encargado del tratamiento que: atiendan las peticiones de los interesados sobre el ejercicio de sus derechos sobre el tratamiento; las operaciones de tratamiento sigan las pautas marcadas en la normativa de protección de datos; y comunique al interesado cualquier violación de la seguridad de sus datos personales.

- Ordenar la rectificación o supresión de los datos personales y la limitación del tratamiento para el cumplimiento de los derechos del afectado, así como la notificación de estas medidas a quienes se les haya comunicado estos datos personales.

- Ordenar que se interrumpa el movimiento de datos hacia un destinatario ubicado en un tercer país o hacia una organización internacional.

Y los poderes de autorización y consultivos son los siguientes:

- Aconsejar al responsable del tratamiento cuando haya habido una consulta previa debida a un posible alto riesgo en el tratamiento de datos.

- Emitir dictámenes en materia de protección de datos personales y aprobar proyectos de códigos de conducta cuando estos ofrezcan las garantías adecuadas.

- Expedir certificaciones y aprobar criterios de certificación, así como acreditar los organismos de certificación.

- Adoptar cláusulas contractuales tipo sobre el tratamiento de protección de datos.

- Aprobar normas corporativas vinculantes que concedan, a los interesados, derechos referentes al tratamiento de sus datos personales.

- Autorizar un tratamiento de datos cuyo responsable ejerza una tarea de interés público que requiera una consulta y autorización previa para llevarse a cabo.

- Autorizar tanto los acuerdos administrativos como las cláusulas contractuales sobre transferencias internacionales de datos que aseguren garantías adecuadas en materia de protección de datos.

8.4 Presidencia

Antes, el encargado de dictar las resoluciones, circulares y directrices de la Agencia de Protección de Datos, así como de dirigirla y representarla, era únicamente el director, que trabajaba con plena independencia y objetividad, sin estar sujeto a instrucciones de nadie, aunque debía escuchar las propuestas del Consejo Consultivo sobre el ejercicio de sus funciones. Ahora, sin embargo, esas funciones las llevan a cabo la Presidencia de la Agencia Española de Protección de Datos y su Adjunto.

El Ministerio de Justicia realiza una propuesta de candidatos al Gobierno, para que el Consejo de Ministros nombre, mediante real decreto, a la Presidencia de la Agencia Española de Protección de Datos y a su Adjunto. Todos esos candidatos son personas expertas en materia de protección de datos.

El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos dura 5 años, uno más que el estipulado para el director de la Agencia de Protección de Datos en la Ley Orgánica de Protección de Datos de Carácter Personal de 1999. Este mandato se puede renovar para otro periodo de la misma duración.

Las situaciones que pueden provocar el cese del mandato de la Presidencia y de su Adjunto antes de que expire son las siguientes:

- Si la Presidencia o su adjunto renuncian mediante petición propia.

- Si el Consejo de Ministros lo exige debido a: un incumplimiento grave de las obligaciones de la Presidencia o su Adjunto, una incapacidad de la Presidencia o su Adjunto para ejercer su función, incompatibilidad, o una condena firme por delito doloso.

Cuando quedan 2 meses para que finalice el mandato o inmediatamente, en caso de cese previo a la expiración del mandato, el Ministerio de Justicia ordena que se publique la convocatoria de candidatos en el Boletín Oficial del Estado. Después, se realiza una evaluación de las aptitudes de los candidatos y el Gobierno hace una propuesta de candidatos al Congreso de los Diputados acompañada de un informe justificativo que debe ser validado por la Comisión de Justicia en votación pública. Para que sea válida, en la primera votación debe ser aceptada por tres quintos de los miembros y si no se alcanzarse ese resultado se debe realizar, inmediatamente después, una segunda votación por mayoría absoluta en la cual los votos favorables procedan de los Diputados que pertenezcan a dos grupos parlamentarios diferentes.

Por último, otra cosa que hay que tener en cuenta es, que tal y como dice el artículo 48.6 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018, los actos y disposiciones dictados por esta Presidencia ponen fin a la vía administrativa y, por lo tanto, se pueden recurrir ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

8.5 Consejo Consultivo

El Consejo Consultivo se encarga de asesorar a la Presidencia de la Agencia Española de Protección de Datos, y consta de los siguientes miembros citados del artículo 49 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018:

- Un Diputado, propuesto por el Congreso de los Diputados.

- Un Senador, propuesto por el Senado.

- Un representante designado por el Consejo General del Poder Judicial.

- Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.

- Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.

- Un experto propuesto por la Federación Española de Municipios y Provincias.

- Un experto propuesto por el Consejo de Consumidores y Usuarios.

- Dos expertos propuestos por las Organizaciones Empresariales.

- Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.

- Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos, propuesto por el Ministro de Justicia.

- Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.

- Un representante de las organizaciones que agrupan a los Consejos Generales Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.

- Un representante de los profesionales de la seguridad de la información propuesto por la asociación de ámbito estatal con mayor número de asociados.

- Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.

- Dos expertos propuestos por las organizaciones sindicales más representativas.

Solo pueden considerarse expertos aquellos que acrediten conocimiento especializado en el Derecho y la práctica sobre protección de datos a través del ejercicio profesional o académico.

Este consejo debe reunirse cuando ordene la Presidencia de la Agencia Española de Protección de Datos, como mínimo una vez cada semestre.

Por último, es necesario tener en cuenta que las decisiones del Consejo Consultivo no poseen carácter vinculante.

8.6 Personal competente de las labores de investigación y los planes de auditoría preventiva

La labor de investigación la realizan funcionarios de la Agencia Española de Protección de Datos o funcionarios externos a ella habilitados por su Presidencia, todos estos funcionarios son considerados agentes de la autoridad en el ejercicio de sus funciones y deben mantener en secreto todos los datos obtenidos durante este ejercicio.

Y en caso de realizar una investigación junto a una autoridad de control perteneciente a otro Estado Miembro de la Unión Europea, el personal de esta autoridad tiene que seguir lo dispuesto en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

8.7 Deber de colaboración

Todo particular o Administración Pública tiene la obligación de proporcionar a la Agencia Española de Protección de Datos la información necesaria para que realicen sus funciones.

Antes de realizar la investigación, si no ha sido posible identificar a los responsables cuya conducta haya podido incumplir la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 y el Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá obtener, de las Administraciones Públicas, la información necesaria para identificarlos.

Además, si no se ha podido llevar a cabo la identificación y la conducta se ha realizado a través de un servicio de la sociedad de la información o una comunicación electrónica, la Agencia Española de Protección de Datos puede obtener información de los prestadores de servicios de la sociedad de la información y de los operadores que presten servicios de comunicaciones electrónicas. La información que puede obtener para la labor de identificar al presunto culpable depende del medio a través del cual se haya realizado la conducta.

Por un lado, si se realiza por medio de un servicio de telefonía, los datos que puede recabar son: el número de teléfono que realizó la llamada; la confirmación de que esa llamada se llevó a cabo; y el nombre completo, número de identificación y dirección del propietario de ese número de teléfono.

Por otro lado, si se realiza por medio de un servicio de la sociedad de la información, los datos que puede recabar son: la fecha, hora e identificación de la dirección IP mediante la cual se realizó la conducta; el nombre completo, número de identificación y dirección del usuario que tenga asignada la dirección IP mencionada previamente; y si la conducta se realizó por correo electrónico, la identificación de la dirección IP desde la que se creó la cuenta de correo a través de la cual se llevó a cabo la conducta, así como la fecha y hora en la que fue creada.

Las cesiones de datos mencionadas en este apartado se pueden llevar a cabo sin autorización judicial cuando el origen de la investigación sea una denuncia por parte del afectado respecto a una mala conducta o al uso de sistemas que permitan divulgar datos personales sin restricciones, para el resto de los casos, se requiere una autorización judicial previa otorgada conforme a las normas procesales.

Para finalizar el apartado sobre el deber de colaboración, hay que tener en cuenta la excepción sobre unos determinados datos de tráfico citada textualmente de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales:

> *Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.*

8.8 Alcance de la actividad de investigación

Los funcionarios que llevan a cabo la investigación pueden realizar ciertas actividades para finalizar con éxito su labor. Algunas de estas tareas ya estaban presentes en el artículo sobre la potestad de inspección de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 y son las siguientes:

- Solicitar el envío o exhibición de documentos y datos.

- Inspeccionar los documentos y datos en el sitio en el que estén guardados.

- Examinar los equipos utilizados para el tratamiento de datos. Para realizar esta tarea cuentan con el acceso a los locales donde están instalados estos equipos.

Además de las tareas mencionadas, también pueden realizar las siguientes actividades:

- Obtener una copia de los datos y documentos.

- Solicitar la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

- Acceder al domicilio constitucionalmente protegido del inspeccionado, siempre que hayan obtenido previamente una autorización judicial para ello o el consentimiento del inspeccionado.

En el caso de que sea necesario inspeccionar órganos u oficinas judiciales, la inspección se llevara a cabo por el Consejo General del Poder Judicial.

8.9 Planes de auditoría

Para analizar el cumplimiento de la vigente normativa de protección de datos personales, la Presidencia de la Agencia Española de Protección de Datos puede iniciar planes de auditoría sobre un sector específico. Estos planes de auditoría consisten en un conjunto de actividades de investigación en materia de protección de datos personales.

Como resultado de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos elabora una serie de normas y se las comunica a un responsable o encargado del tratamiento para que las siga con el objetivo de asegurar el cumplimiento del Reglamento (UE) 2016/679, así como de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

Para la elaboración de estas normas de cumplimiento obligatorio, la Presidencia puede colaborar con los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos existentes.

8.10 Potestades de regulación

La Presidencia de la Agencia Española de Protección de Datos tiene la potestad de regulación para dictar disposiciones sobre protección de datos denominadas “Circulares de la Agencia Española de Protección de Datos”. La elaboración de estas circulares está sujeta a lo dispuesto en el Estatuto de la Agencia Española de Protección de datos.

Las Circulares de la Agencia Española de Protección de Datos son obligatorias a partir del momento en el que se publican en el Boletín Oficial del Estado.

8.11 Acción Exterior

A la Agencia Española de Protección de Datos le compete la titularidad y el ejercicio de las funciones sobre protección de datos que tengan que ver con la acción exterior del Estado. Respecto a la acción exterior, la Agencia Española de Protección de Datos:

- Protege a las personas físicas en tratamientos de datos que surgen de algún Convenio Internacional en el que participe España.

- Participa en reuniones y foros internacionales fijados en un pacto entre las autoridades de control de protección de datos personales.

- Proporciona información a las autoridades autonómicas de protección de datos sobre las decisiones tomadas en el Comité Europeo de Protección de Datos y obtiene su opinión en los asuntos que le competan.

- Participa en las organizaciones internacionales en materia de protección de datos y en grupos de trabajo o foros internacionales.

- Colabora con entidades de otros Estados con el objetivo de impulsar, promover y desarrollar el derecho fundamental de protección de datos.

Además, mediante las autoridades autonómicas de protección de datos, a las comunidades autónomas les corresponde:

- Desempeñar las funciones como sujetos de la acción exterior en el marco de sus competencias.

- Realizar tanto acuerdos internacionales administrativos para un tratado internacional, como acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, sin obligación jurídica para quienes los firmen.

9. Anexo E: Delegado de Protección de Datos

En la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018 se añade la figura del delegado de protección de datos cuyas funciones son, básicamente, realizar un asesoramiento en materia de protección de datos, actuar como intermediario entre la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, supervisar el cumplimiento de la normativa de protección de datos y atender reclamaciones.

9.1 Cualificación

Para que un delegado sea seleccionado, este debe ser apto para el cargo y por lo tanto se comprueban sus cualidades profesionales. Las cualidades que más se valoran son:

- Sus conocimientos sobre el Derecho y la práctica en materia de protección de datos.

- Su capacidad para informar y asesorar a los que intervengan en el tratamiento sobre las obligaciones que les atañen en materia de protección de datos.

- Su talento para supervisar el cumplimiento de las políticas del responsable o encargado del tratamiento sobre la protección de datos personales, así como el cumplimiento de la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales de 2018.

- Su disposición para el asesoramiento de la evaluación de impacto.

- Su aptitud para cooperar con la autoridad de control, o actuar como punto de contacto de esta para temas relativos al tratamiento y realizar consultas sobre cualquier otro asunto.

Estas cualidades son demostrables, para ello se puede hacer uso de mecanismos de certificación que toman muy en consideración la posesión de un título universitario que demuestre conocimientos especializados en el derecho y la práctica sobre protección de datos.

9.2 Posición

El delegado actúa como interlocutor ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, y puede inspeccionar procedimientos y emitir recomendaciones.

Cuando el delegado de protección de datos sea una persona física de la organización del responsable o encargado del tratamiento, estos no podrán removerlo ni sancionarlo por llevar a cabo sus funciones, a no ser que realice una estafa o una negligencia grave en el ejercicio. Es

necesario que exista la independencia del delegado dentro de la empresa, evitando cualquier conflicto de intereses.

El delegado puede acceder a los datos personales y procesos del tratamiento para cumplir con sus funciones, y el responsable o encargado de este tratamiento no puede negarle el acceso escudándose en el deber de confidencialidad o secreto.

En caso de que el delegado se entere de una vulneración con relación a la protección de datos, este debe comunicárselo de inmediato a los órganos de administración y dirección del responsable o encargado del tratamiento para que tomen las medidas oportunas.

9.3 Intervención en las reclamaciones

El delegado tiene dos formas de actuar ante una reclamación:

- Cuando el afectado decida contactar con él antes de presentar reclamaciones contra el responsable o el encargado del tratamiento, el delegado tendrá un plazo de dos meses para comunicar al afectado la decisión adoptada.

- Cuando la Agencia Española de Protección de Datos o la autoridad autonómica de protección de datos correspondiente, tras recibir una reclamación por parte de un afectado, contacte con el delegado para que tome las medidas que considere oportunas en el plazo de un mes. Si durante este plazo, el delegado no se hubiera comunicado con ellos para dar respuesta a la reclamación, esta autoridad seguirá el proceso en base a lo establecido en el apartado 2.11, sobre los procedimientos en caso de una posible vulneración de la normativa de protección de datos, de este documento.

Todo proceso ante la Agencia Española de Protección de Datos seguirá lo dispuesto en el apartado 2.11, sobre los procedimientos en caso de una posible vulneración de la normativa de protección de datos, de este documento. Además, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

10. Glosario de términos

Relación contractual: es un acuerdo legal entre varias partes que cuenta con derechos y responsabilidades para los partícipes.

Sistemas de información crediticia: son sistemas en los que se incluyen a todas las personas que no hayan pagado una deuda en el plazo estipulado.

Resolución motivada: es un acto administrativo que resuelve y finaliza la vía administrativa y en el que se explican las razones de este acto.

Anonimización: es el proceso de separar la identidad de la persona de sus otros datos, de manera que no se pueda identificar a la persona a la cual hacen referencia estos datos.

Seudonimización: es el proceso de cambiar datos personales identificativos por seudónimos, de manera que se pueda realizar el tratamiento de datos sin la necesidad de usar los datos que identifiquen al interesado, pero sin desvincularlos.

LOPD: Ley Orgánica de Protección de Datos (1999).

LOPDD: Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (2018).

ISP: Proveedor de servicios de internet.

Normas corporativas vinculantes: son reglas aplicables a una empresa o unión de empresas para ofrecer garantías en materia de protección de datos tras una transferencia internacional de datos a un destinatario de un país que no tenga un nivel de seguridad adecuado.

Brecha de seguridad: es un incidente que afecta a los datos personales.

11. Bibliografía

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
  https://www.boe.es/eli/es/lo/1999/12/13/15

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  https://www.boe.es/eli/es/lo/2018/12/05/3/con

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo
  https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

- Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
  https://www.boe.es/eli/es/l/2014/06/26/10/con

- Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.
  https://www.boe.es/eli/es/lo/1985/06/19/5/con

- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
  https://www.boe.es/eli/es/l/2000/01/07/1/con

- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
  https://www.boe.es/eli/es/l/2002/11/14/41/con

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
  https://www.boe.es/eli/es/l/2013/12/09/19/con

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
  https://www.boe.es/eli/es/l/2015/10/01/39/con

- Principio de Accountability. El papel del DPD. Impulso de los Códigos de Conducta. (Julián Prieto Hergueta)
  https://www.aepd.es/agencia/transparencia/jornadas/common/10-sesion/5-julian-prieto.pdf

- Los códigos de conducta: una poderosa herramienta de cumplimiento del RGPD. (Equipo PSN Sercon)
  https://blog.psnsercon.com/los-codigos-de-conducta-una-poderosa-herramienta-de-cumplimiento-del-rgpd/

- Guía para la gestión y notificación de brechas de seguridad. (Agencia Española de Protección de Datos)
  https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

- La regla 3-2-1: una gran técnica para tus copias de seguridad. (Mediacloud)
  https://blog.mdcloud.es/regla-3-2-1-copias-seguridad/

- Guía sobre borrado seguro de la información. Una aproximación para el empresario. (Instituto Nacional de Ciberseguridad)
  https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad_0.pdf

- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. (Agencia Española de Protección de Datos)
  https://www.aepd.es/media/guias/guia-directrices-contratos.pdf