AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

LISTADO DE CUMPLIMIENTO NORMATIVO

INTRODUCCIÓN

En las Guías de Análisis de Riesgos y Evaluaciones de Impacto publicadas por la Agencia Española de Protección de Datos (AEPD) se cita textualmente el Considerando 74, que establece que *"….el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas*".

Con base en lo anterior, se deduce la importancia de identificar las amenazas y riesgos a los que está expuesta una actividad de tratamiento de datos personales, por lo que se considera fundamental disponer de una descripción detalla del mismo, su contexto y los elementos más relevantes que intervienen para poder gestionar los riesgos con el fin de minimizarlos al máximo.

El proceso de gestión de riesgos implica realizar inicialmente dos tareas: identificarlos y evaluarlos. En consecuencia, es muy importante asegurar una correcta identificación de las amenazas a los que está expuesta una actividad de tratamiento teniendo en cuenta que entre los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas se pueden diferenciar dos dimensiones: riesgos asociados a la protección de la información con el foco central en la integridad, disponibilidad y confidencialidad de los datos y riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

El listado de cumplimiento normativo que se recoge a continuación se encuentra referenciado en las citadas guías y puede ser utilizado por responsables y encargados de tratamientos de datos personales como un método básico que les va a permitir identificar los requisitos de cumplimiento del Reglamento General de Protección de Datos (RGPD) con el objeto de poder valorar los aspectos que deben tener en cuenta durante los procesos de análisis de riesgos y evaluación de impacto. Además, puede suponer una ayuda en las tareas de supervisión y asesoramiento que llevan a cabo los Delegados de Protección de Datos.

Este recurso se suma a los publicados por la AEPD relacionados con el enfoque de riesgos del RGPD, incluyendo aquellas entidades que tratan datos personales de escaso riesgo para los derechos y libertades de las personas y que se benefician de la herramienta FACILITA.

Es importante destacar que este listado recoge aspectos que deben ser tenidos en cuenta desde el diseño de un tratamiento de datos, además de ser de utilidad para verificar el nivel de cumplimiento del RGPD de cualquier organización, de forma que se puedan implantar los controles necesarios a fin de garantizar la proactividad que el Reglamento exige a responsables y encargados de tratamientos. El uso de este documento muestra una visión general de los aspectos en los que es necesario incidir con el fin de garantizar la licitud del tratamiento o mejorar aspectos relacionados, por ejemplo, con la transparencia y la información que se facilita a los interesados.

Es preciso señalar la necesidad de mantener documentados todos los procesos, en especial en lo que se refiere a la identificación del riesgo relacionado con el tratamiento y la evolución del mismo, con el objetivo de acreditar la diligencia en el cumplimiento del RGPD. En este sentido, además de otros documentos que fueran necesarios, el análisis que pudiera llevarse a cabo mediante este documento debería formar parte de dicha base documental de manera que permita a responsables y encargados demostrar en cualquier momento su diligencia y proactividad con relación con el cumplimiento normativo de los tratamientos que llevan a cabo.

Finalmente, se muestra la tabla en la que se describen las cuestiones mínimas de obligado cumplimiento a tener en cuenta en los tratamientos de datos según lo previsto en el articulado del RGPD. Se trata de una lista de verificación con la que puede llevarse a cabo la comprobación del grado de cumplimiento normativo y cada organización debe interpretar el resultado obtenido, abordando las posibles deficiencias que hubieran sido detectadas.

El mero uso de este u otros recursos de ayuda facilitados por la Agencia Española de Protección de Datos no implica necesariamente el cumplimiento del RGPD.

LISTADO DE CUMPLIMIENTO DEL RGPD	*CUMPLE SI / NO*

PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	
Se mantiene la trazabilidad de los fines del tratamiento	

LICITUD DEL TRATAMIENTO	
Se tiene consentimiento para cada finalidad del tratamiento	
El tratamiento es necesario para ejecutar un contrato o precontrato	
Existe obligación legal	
El tratamiento es necesario para proteger intereses vitales	
El tratamiento es necesario para el cumplimiento de interés público	
El tratamiento es necesario para satisfacer intereses legítimos	

CONDICIONES PARA EL CONSENTIMIENTO	
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	
Se solicita el consentimiento de forma inteligible y de fácil acceso	
Se solicita usando lenguaje claro y sencillo	
Se informa con carácter previo a recabar el consentimiento	
Se permite retirar el consentimiento con la misma facilidad que se recaba	
Se ofrecen medios para retirar el consentimiento en cualquier momento	
Se recaba el libre consentimiento	

Para prestar un servicio se solicitan sólo los datos necesarios	
Para ejecutar un contrato se solicitan sólo los datos necesarios	

CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN	
Se recaba el consentimiento de menores de 14 años al titular de la patria potestad o tutela sobre el niño	
Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño	

TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS	
Se tratan los datos sólo cuando existen normas que lo exceptúen	
Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho	
Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical)	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados	
Se tratan datos que el interesado ha hecho manifiestamente públicos	
Es necesario para la formulación, el ejercicio o la defensa de reclamaciones	
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	
Es necesario por razones de interés público en el ámbito de la salud pública sobre la base normas de Derecho que establece medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional	
Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho	
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	

TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES	
Se tratan los datos bajo la supervisión de las autoridades públicas	
Se tratan los datos bajo la autorización de normas de derecho	
El registro completo de condenas penales se realiza bajo el control de las autoridades públicas	

TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN	
Se mantiene información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	
Se obtiene y/o trata información adicional con vistas a identificar al interesado cuando los fines no requieren esa identificación	
Se puede demostrar que los datos anonimizados no permiten identificar a los interesados	
Se informa al interesado y se recaba su consentimiento cuando se llega a su identificación	
Se cancelan los datos cuando se llega a identificar al interesado	

DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN	
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	
La información se facilita de forma concisa, transparente e inteligible	
La información se facilita en lenguaje claro y sencillo	
Se facilita por escrito o por otros medios, incluidos los electrónicos	
Se facilita verbalmente, previa acreditación de su identidad	
Se facilita al interesado el ejercicio de sus derechos	
Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	
Se informa al interesado en el plazo de un mes desde la recepción de su solitud	
Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud	
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	
Se permite a los interesados el ejercicio de derechos por medios electrónicos	
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud	
Se facilita gratuitamente el ejercicio de derechos	
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	

DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO	
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	
Se facilitan los datos de contacto del delegado de protección de datos	
Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento	
Se facilita información sobre el interés legitimo	
Se informa sobre los destinatarios o las categorías de destinatarios	
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	
Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se informa de las cesiones basadas en requisitos legales o contractuales	
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	
Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento	
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	

DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO	
Se informa de la identidad y los datos de contacto del responsable y, en su caso, de su representante	
Se informa de los datos de contacto del DPD	
Se informa de los fines del tratamiento	
Se informa de la base jurídica del tratamiento	
Se informa de las categorías de datos personales de que se trate	
Se informa de los destinatarios o las categorías de destinatarios de los datos	
Se informa del plazo durante el cual se conservarán los datos personales	
Se informa de los criterios utilizados para determinar este plazo el plazo de conservación cuando no es posible informar del mismo	
Se informa de los intereses legítimos concretos en que se basa el tratamiento	
Se informa del derecho a solicitar el acceso a sus propios datos personales	
Se informa del derecho a solicitar la rectificación de sus datos	
Se informa del derecho a solicitar la supresión	
Se informa del derecho a la limitación del tratamiento	
Se informa del derecho a oponerse al tratamiento	
Se informa del derecho a la portabilidad de los datos	
Se informa de la existencia del derecho a retirarlo el consentimiento en cualquier momento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se informa de la fuente de la que proceden los datos personales	
Si proceden de fuentes de acceso público, se informa de ello	
Se proporciona la información antes de un mes	
Si los datos personales se utilizan para comunicación con el interesado, se le comunica la información a que tiene derecho en el momento de la primera comunicación	
Si está previsto comunicar los datos personales del interesado a otro destinatario, se le comunica la información a más tardar en el momento en que los datos personales son comunicados por primera vez	
Se informa al interesado si se realizan tratamientos para finalidades diferentes de la que fueron recogidos	
No se informa cuando ya dispone de la información el interesado	
No se informa cuando la comunicación de dicha información resulta imposible o supone un esfuerzo desproporcionado	
No se informa porque puede imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento pero se adoptan medidas para proteger los derechos, libertades e intereses legítimos del interesado	
No se informa porque la obtención o la comunicación está expresamente establecida por normas de derecho aplicables	
No se informa porque los datos personales tienen carácter confidencial sobre la base de una obligación de secreto profesional regulada por normas de Derecho	

DERECHOS DEL INTERESADO. DERECHO DE ACCESO	
Se informa respecto a los fines del tratamiento	
Se informa de las categorías de datos personales que se tratan	
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	
Se informa del plazo previsto de conservación de los datos personales	
Se informa de los criterios utilizados para determinar el plazo de conservación	
Se informa del derecho a solicitar la rectificación o supresión de sus datos	

Se informa del derecho a solicitar la limitación del tratamiento de los datos	
Se informa del derecho a solicitar la oposición al tratamiento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio	

DERECHOS DEL INTERESADO. DERECHO DE RECTIFICACIÓN	
Se rectifican los datos personales inexactos sin dilación indebida	
Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento	

DERECHOS DEL INTERESADO. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)	
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	
Se suprimen los datos cuando se opone al tratamiento	
Se suprimen los datos cuando han sido tratados ilícitamente	
Se suprimen los datos cuando lo exige una obligación legal	
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	

DERECHOS DEL INTERESADO. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO	
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso	
Se limita el tratamiento cuando no son necesarios para los fines pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones	
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	
Se informa al interesado cuando se levanta la limitación del tratamiento	

INFORMACIÓN AL INTERESADO ANTE RECTIFICACIÓN, SUPRESIÓN O LIMITACIÓN EN EL TRATAMIENTO	
Se comunican al interesado la rectificación, supresión o limitación en el tratamiento	

DERECHOS DEL INTERESADO. DERECHO A LA PORTABILIDAD DE LOS DATOS	
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica	
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato	
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	
Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente	

DERECHOS DEL INTERESADO. DERECHO DE OPOSICIÓN	
Se atienden las solicitudes de oposición y se dejan de tratar los datos	
Se atienden las solicitudes de oposición pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	
Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados	

DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES	
No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	
Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	

RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO	
Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD	
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	
Se aplican medidas técnicas y organizativas apropiadas	
Las medidas se revisan y actualizan cuando es necesario	
Se han confeccionado políticas de protección de datos	
Se aplican las políticas de protección de datos	

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO	
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento	
Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	
Durante el tratamiento se aplican las medidas que han sido determinadas	
Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	
Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad	
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	

CORRESPONSABLES DEL TRATAMIENTO	
Se han determinado de modo transparente, y de mutuo acuerdo, las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD	
El acuerdo fija las respectivas obligaciones de suministro de información al interesado	
El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados	
Los aspectos esenciales del acuerdo están a disposición del interesado	

ENCARGADO DEL TRATAMIENTO	
Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado	
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	
El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos del responsable	
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable	
El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria	
El contrato establece que se tomarán las medidas de seguridad necesarias	
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	
El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados	
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	
El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable	
El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho	
El contrato consta por escrito	
Sólo se accede a los datos siguiendo instrucciones del responsable	

REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	
Se lleva un registro de las actividades de tratamiento	
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	
El registro recoge los fines del tratamiento	
Recoge una descripción de las categorías de interesados y de las categorías de datos personales	
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	
Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	
Incluye los plazos previstos para la supresión de las categorías de datos	
Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	

SEGURIDAD DEL TRATAMIENTO	
Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	
Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	
Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	

NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL	
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas	
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	
Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	
Se documenta cualquier brecha de seguridad de los datos personales	
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	
Se ha comprobado que el procedimiento de notificación funciona	

COMUNICACIÓN DE UNA BRECHA AL INTERESADO	
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades	
La comunicación al interesado, se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	

EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS	
Se recaba el asesoramiento del DPD	
Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	
La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido	
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	
La EIPD incluye una evaluación de los riesgos para los derechos y libertades	
Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas	
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	
Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo	
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	
Se informa de los fines y medios del tratamiento previsto en la consulta	
Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	
Se facilitan los datos de contacto del delegado de protección de datos	
Se incluye la evaluación de impacto	
Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control	

DELEGADO DE PROTECCIÓN DE DATOS	
Se ha designado un DPD por requerimiento legal	
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	
Se da respaldo en el desempeño sus funciones	
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento	
Se le facilitan los recursos necesarios para mantener sus conocimientos	
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	
El DPD rinde cuentas directamente al más alto nivel jerárquico	
El DPD atiende las solicitudes de los interesados	
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	

El DPD coopera y actúa como punto de contacto con la autoridad de control	

TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES	
Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de nivel de protección adecuado por la Comisión Europea	
Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea	
Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales.	
Existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos	
Existen normas corporativas vinculantes	
Existen cláusulas tipo de protección de datos adoptadas por la Comisión	
Existen cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión	
Existe un código de conducta junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existe un mecanismo de certificación junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existen cláusulas contractuales que requieren la autorización previa de la autoridad de control	
Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados	
Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas	
Se dispone del consentimiento explícito del interesados y se le ha informado de los posibles riesgos	
Son necesarias para la ejecución de un contrato con el interesado o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado	
Son necesarias para la formulación, ejercicio o la defensa de reclamaciones	
Son necesarias para la protección de los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento	
Por intereses legítimos imperiosos	
Afecta a un número limitado de interesados y no es repetitiva	
Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantías apropiadas	
Se ha informado a la autoridad de control