Crue-Secretarías Generales

Comision Delegada del grupo de Trabajo de Delegadas y Delegados de Protección de Datos

Guía orientativa para la formalización de encargos de tratamiento de datos personales en el ámbito universitario

*Como citar este informe:

Guía orientativa para la formalización de encargos de tratamiento de datos personales en el ámbito universitario

Este documento de trabajo responde exclusivamente a las opiniones de sus autores

FECHA Febrero 2024

Grupo de Trabajo Delegadas y Delegados de Protección de Datos.

Universidades participantes:

Universidad Alfonso Décimo el Sabio	David Díaz
Universidad Burgos	Aída Rodríguez
Universidad Católica de Valencia	Paula Royo
Universidad de Granada	Mª Del Carmen García
Universidad Pompeu y Fabra	Marc Vives
Universidad Pública de Navarra	Javier Zazu
Universidad de Sevilla	Margarita Martínez-Pais

Contenido

Alcance de la presente Guía

La Guía está dirigida a delegados de protección de datos de Universidades, los cuales, dentro de las funciones atribuidas por el artículo 39 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, RGPD), lleven a cabo funciones de asesoramiento, supervisión y control de tesis doctorales, trabajos fin de titulación u otros trabajos académicos (en adelante, la actividad o actividades). Por tanto, se omitirá información y explicaciones que, atendiendo a su ámbito de conocimiento, se entienden como adquiridas.
Como documento complementario a esta Guía, se aporta un manual o documento destinado a aquellas personas que realicen este tipo de actividades, cuyo fin es pedagógico y de concienciación, evitando utilizar en exceso terminología jurídico-técnica que pueda confundir al lector, tratando de apoyar cada uno de los apartados en ejemplos prácticos

¡AVISO!

Este documento se pone a disposición de los delegados de protección de datos, para que la misma pueda ser utilizada a su libre criterio, sólo sirviendo como base o ejemplo en la forma de proceder. Su contenido no vincula a los delegados de protección de datos de las universidades, los cuales tienen independencia en el ejercicio de las funciones de asesoramiento y supervisión que les establece la normativa de protección de datos personales.

1 Objeto

El objeto del presente documento es ofrecer una guía práctica al personal de las Universidades sobre formalización de encargos de tratamiento de datos personales en contratos y convenios con terceros, conforme a:

1. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD); Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
2. Los criterios de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos.
3. La Guía del Comité Europeo de Protección de Datos sobre responsables y encargados
4. La Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, en el caso de las universidades públicas
5. La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el caso de las universidades públicas
6. Legitimación civil y mercantil que resulte de aplicación, en el caso de las universidades privadas.

2 Alcance

La presenta Guía ofrece información práctica para:

a) gestores de la contratación en todos los niveles
b) equipos que se integren en consorcios de investigación
c) investigadores que operen bajo contrato como encargado del tratamiento
d) unidades de gestión que presten servicios a terceros en calidad de encargado del tratamiento (alojamiento de websites de congresos, provisión de medios a sindicatos, centros adscritos, servicios de alquiler de aulas con personal de soporte en control de asistencia, prestación de servicios científico-técnicos a terceros …)
e) Medios propios

3 Finalidad de la Guía

La finalidad de la guía es:

▪ Promover una cultura de cumplimiento y, en particular, en el ámbito de la contratación y de la formalización de convenios de colaboración.
▪ Integrar los procesos de cumplimiento en los procesos de gestación, definición y ejecución de contratos y convenios de colaboración.
▪ Promover estrategias de cumplimiento coordinado en la gestión descentralizada de la contratación menor.
▪ Asegurar el cumplimiento de los medios propios.

4 Destinatarios

La presente guía está dirigida a todo aquel empleado de la Universidad que forme parte del proceso de contratación o formalización de convenios.
En concreto;

▪ Unidades de contratación.
▪ Oficina de convenios.
▪ Unidades con competencia en la contratación menor.
▪ Unidades con competencia en formalización de convenios de colaboración.
▪ Asesorías jurídicas.
▪ OTRI y servicios de investigación o transferencia.
▪ Personal investigador que actúe en calidad de encargado.
▪ Medios propios.
▪ Personas delegadas de protección de datos
▪ Responsables de seguridad
▪ Centros (Facultades y Escuelas de posgrado y doctorado)

- Servicios de estudiantes, estudios, grado, posgrado y doctorado.
- Servicios TI.

5 ¿Qué es un encargo del tratamiento?

La Universidad como Institución con personalidad jurídica propia, necesita en el marco de sus funciones y competencias contratar con distintas empresas prestadoras de servicios.

Esta prestación de servicios por parte de colaboradores externos tiene repercusión en el ámbito de la protección de datos personales, pues puede implicar que dichos colaboradores traten datos personales con respecto a los cuales, la Universidad es responsable frente a los titulares o interesados.

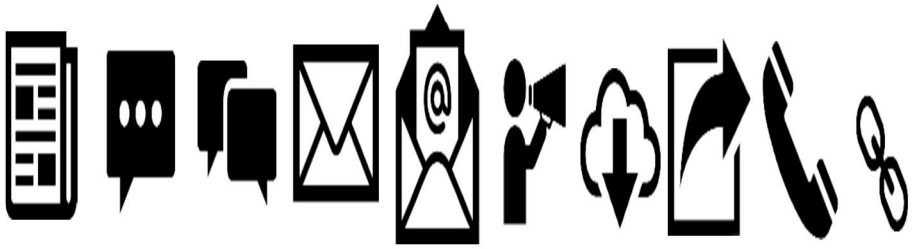
Se habla así, de un encargado del tratamiento (colaborador externo prestador del servicio) y de responsable del tratamiento (Universidad).

La relación jurídica entre ambos sujetos (Universidad y colaborador externo prestador de un servicio), en lo referido al tratamiento de datos personales a realizar, debe instrumentarse necesariamente y por imperativo legal mediante un contrato; Surge así la necesidad de suscribir el **CONTRATO DE ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES**.

Con carácter previo, es necesario tener presentes las siguientes definiciones (Extraídas del **artículo 4 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO Y DEL CONSEJO EUROPEO**, *de ahora en adelante, **RGPD**):*

DATOS PERSONALES: "*Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*".

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



RESPONSABLE DEL TRATAMIENTO: *"La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".*

ENCARGADO DEL TRATAMIENTO: *"La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Sería la empresa contratista, que realizará bajo nuestras instrucciones el tratamiento de datos personales en cuestión". Nos referimos a encargo del tratamiento cuando una entidad (Responsable del Tratamiento), acuerda con otra (Encargado del Tratamiento) la prestación de un servicio por el cuál es necesario que el Encargado trate datos personales de los que sea responsable la primera.*

Con carácter orientativo, se recoge a continuación un glosario orientativo de **posibles actividades de tratamiento:**

Recogida (captura de datos). - se trata de la recopilación de datos, ya sea manual o de forma automatizada, mediante formularios, encuestas, entrevistas, etc.
Registro (grabación). - cualquier actividad encaminada a la inscripción, anotación o asiento en algún soporte, digital o no, de datos personales.
Estructuración. - operación con la que se pretende organizar un conjunto de datos según un patrón y objetivo determinado.
Modificación. - consiste en cambiar el contenido o parte de éste, de algún dato, porque haya que actualizarlo desde que se recopiló.
Conservación (almacenamiento). - uso de medios de registro para mantener los datos personales en soportes físicos o digitales garantizando su disponibilidad por el usuario.
Extracción. - consiste en recabar datos de distintas fuentes con vistas a realizar un procesamiento o almacenamiento posterior.
Consulta. - permitir que personas autorizadas puedan examinar los datos contenidos en cualquier soporte.
Cesión o comunicación. - la revelación de datos realizada a una persona distinta de la persona física de la que se recabó, sin que, a diferencia de la difusión, pueda hacerse público a terceros ajenos a la relación contractual o de cooperación entre autoridades o administraciones públicas.
Difusión. hacer públicos los datos personales a terceros ajenos a la relación contractual, siempre que esté contemplado y se ajuste a la legalidad vigente.
Interconexión (cruce). - garantizar la disponibilidad de los datos personales para el intercambio con otra fuente o plataforma que almacene datos.
Cotejo. - posibilidad de contrastar los datos de una fuente o soporte con los de otra fuente o soporte. En ocasiones puede precisarse de interconexión para realizar esta operación.
Limitación. - Adoptar medidas sobre unos datos personales con el objetivo de evitar su modificación, borrado o supresión.
Supresión. - consiste en eliminar definitivamente los datos que puedan estar contenidos en cualquier soporte, de forma que no puedan ser recuperados de estos.
Destrucción. - la destrucción implica inutilizar el soporte, fuente, repositorio, etc. en el que se contenían los datos.
Recuperación. - garantizar la posesión de nuevo de aquellos datos que, por cualquier motivo, sean de la fuente, soporte o debido al formato, no estuvieran disponibles temporalmente.
Duplicado. - realizar una copia idéntica de una serie de datos para ser incluida en otra fuente, base de datos o soporte.
Copia (copias temporales). - realizar copia de datos de forma que estén disponibles, pero de forma limitada para realizar alguna otra operación o tratamiento puntual.
Copia de seguridad. - realizar una copia de datos originales con vocación de reserva, de forma que, ante un imprevisto, se pueda garantizar su recuperación garantizando su integridad.

Por lo general, los contratos que suelen llevar aparejado algún tratamiento de datos personales son los de servicios contratados con terceros. También es posible que la consecución de los objetivos de un convenio implique un encargo de tratamiento de datos personales.

Por ejemplo, contratos para la gestión y mantenimiento de una web en la que se procesen datos personales; la contratación del mantenimiento de una aplicación que, para su finalidad, precise gestionar alguna base de datos personales; la contratación de servicios en la nube; la contratación de una empresa para destrucción o encuadernación de documentos

El Responsable del tratamiento queda obligado a elegir y comprobar que contrata a un encargado que ofrece garantías suficientes para garantizar la protección de los derechos del interesado.
El Encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Ejemplo: la Universidad (en este caso como responsable del tratamiento) contrata a un tercero llamado X (en este caso encargado del tratamiento) para que "imparta unas jornadas de asistencia obligatoria" a su alumnado en su nombre.

Para realizar las jornadas, es necesario que el tercero X (Encargado) registre la asistencia y trate los datos personales del alumnado de la Universidad (Responsable). Sin esos datos, no se puede prestar el servicio contratado.

Previo a su contratación, la Universidad comprueba que la empresa X cumple con las garantías exigidas por la normativa en protección de datos y por tanto va a tratar los datos de su alumnado diligentemente, garantizando la protección de los mismos.

El Responsable del tratamiento es quien se encarga de determinar los fines y medios del tratamiento, y a determinar las directrices que debe seguir el encargado.

Cabe recordar que el Encargado actúa siempre en nombre del Responsable, y no en nombre propio. Si un Encargado del tratamiento decide determinar los fines y medios del tratamiento, será considerado Responsable del tratamiento con respecto a dicho tratamiento.

Ejemplo: Si la entidad X utiliza los datos del alumnado de la Universidad con fines suyos, como puede ser enviar información comercial al alumnado de la Universidad ofreciéndole más jornadas impartidas por dicha entidad y ajenas a la Universidad, pasa a actuar como Responsable del tratamiento, respondiendo como tal.

De igual manera, un Encargado del tratamiento no puede recurrir a otro encargado sin autorización previa del Responsable. En caso de que se permita, y el Encargado subcontrate a un tercero, queda obligado a informar al Responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al Responsable la oportunidad de oponerse a dichos cambios.

Cuando un Encargado del tratamiento recurra a otro encargado, deben firmar un contrato u otro acto jurídico donde consten las mismas obligaciones de protección de datos que las estipuladas en el suscrito entre el Responsable y el Encargado principal. Si ese otro Encargado incumple sus obligaciones de protección de datos, el Encargado principal (la empresa X) seguirá siendo plenamente responsable ante el Responsable del tratamiento (La Universidad) por lo que respecta al cumplimiento de las obligaciones del otro Encargado (la empresa Y).

Ejemplo: La empresa X solo podrá subcontratar a otra empresa (Y) que necesite tratar los datos personales de la Universidad para que le asista en la impartición de las jornadas, con consentimiento expreso de la Universidad.

En caso de que la Universidad lo consienta, la empresa X deberá firmar un contrato u otro acto jurídico con la empresa Y con los mismos términos y obligaciones que el que tiene firmado con la Universidad. Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales.

La relación jurídica entre ambos sujetos (Universidad y colaborador externo prestador de un servicio), en lo referido al tratamiento de datos personales a realizar, **debe instrumentarse necesariamente y por imperativo legal mediante un contrato o acto jurídico con el contenido mínimo establecido en el**

artículo 28 del RGPD. Surge así la necesidad de suscribir el **ENCARGO DE TRATAMIENTO DE DATOS PERSONALES**, objeto de esta *Guía orientativa.*

(Ver **Anexo 1 - Cláusulas de encargo de tratamiento de datos personales)**

Cuando sea de aplicación la normativa aplicable a los contratos del sector público, también será de aplicación el régimen establecido en el RGPD.

Una vez analizados los roles de Responsable y Encargado, cabe mencionar que existe otro supuesto denominado ***CORRESPONSABLE***.

Existen situaciones en las que la universidad puede determinar conjuntamente con otra parte los objetivos y los medios de un tratamiento de datos personales. En este caso se dice que ambas partes actúan como corresponsables del tratamiento.

Ejemplos: un grupo de investigación de la universidad participa en un proyecto europeo los objetivos y medios a utilizar del cual son determinados conjuntamente por todos los 'partners' del proyecto; la Universidad es parte de un máster interuniversitario y participa con las otras universidades participantes en las decisiones académicas sobre el mismo (admisión de candidatos, cualificaciones, emisión de títulos…); etc.

Los tratamientos de datos persones en régimen de corresponsabilidad están regulados en el **artículo 26 del RGPD** y precisan que los corresponsables determinen de modo transparente y mutuo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, en especial la atención al ejercicio de derechos por parte de las personas y las obligaciones de suministro de la información relativa al tratamiento a las mismas.

5.1 ¿Cómo actuar si la Universidad es responsable de un tratamiento de datos personales que conlleva un encargo?

Cuando el contrato/convenio principal implique un encargo de tratamiento de datos personales de la Universidad por parte de una persona o entidad externa, la Universidad deberá cumplir las siguientes obligaciones legales **(artículo 28 RGPD)**, con carácter previo a que el encargado realice el tratamiento de datos por cuenta de la misma:

1. Comprobar que el Encargado de tratamiento ofrece garantías suficientes para cumplir los

requisitos del RGPD y garantizar la protección de los derechos de los interesados.

2. Formalizar el Encargo de tratamiento en un contrato o acto jurídico, donde se concretarán las instrucciones del responsable, a las que se habrá de sujetar el Encargado. Ese contrato o acto jurídico deberá cumplir con el contenido específico, establecido en el **artículo 28.3 del RGPD.**

De conformidad con lo dispuesto en el **artículo 28.1 del RGPD**, el Responsable del tratamiento tiene un deber de diligencia en la selección del Encargado de tratamiento.
Una persona, física o jurídica, ofrecerá garantías suficientes para asumir la función de encargado de tratamiento cuando tenga conocimientos especializados y medidas técnicas, organizativas y de seguridad del tratamiento, para cumplir con los requisitos del RGPD y asegurar una adecuada protección de los derechos de los interesados en materia de protección de datos personales.

Por ejemplo, son indicadores de que el posible encargado de tratamiento ofrece garantías suficientes de protección de los derechos de los interesados (art. 40 RGPD): la adhesión a códigos de conducta en materia de protección de datos; la posesión de un certificado de protección de datos; la certificación del cumplimiento del ENS (Esquema Nacional de Seguridad); o la asunción expresa del compromiso vinculante y jurídicamente exigible de adoptar esas garantías de protección de los derechos de los interesados.

De conformidad con lo dispuesto en el **artículo 28.3 del RGPD**, el encargo de tratamiento podrá formalizarse dentro del clausulado del acuerdo o convenio suscrito entre la Universidad responsable del tratamiento y el encargado que dé lugar al mismo, o bien en un acto jurídico separado, que deberá acompañarse como anexo al primero.

En todo caso, el acto jurídico en el que se formalice el encargo de tratamiento deberá contener las menciones mínimas contempladas en el **artículo 28.3 del RGDP**:

1. Se indicará el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.
2. Además, se recogerán expresamente las siguientes obligaciones del encargado:
    a) *Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo*

que tal Derecho lo prohíba por razones importantes de interés público;

b) *Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;*
c) *Tomará todas las medidas necesarias de conformidad con el artículo 32;*
d) *Respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;*
e) *Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;*
f) *Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;*
g) *A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;*
h) *Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.*

Se recomienda a las Universidades tener modelos básicos de actos jurídicos de Encargo de tratamiento, debidamente supervisados por su Delegado/a de Protección de Datos.
Puede consultar los modelos que figuran en estas Orientaciones como Anexos.
(Ver Anexo 1 - Cláusulas de encargo de tratamiento de datos personales)

5.2 ¿Puede ser encargada del tratamiento la Universidad? ¿En qué supuestos?

La Universidad asumirá la posición de encargado del tratamiento cuando trate datos personales de los que sea responsable una persona o entidad externa, conforme a los fines e instrucciones establecidos por ésta.
Así ocurrirá cuando una empresa, entidad u organización encomiende a personal, unidades o servicios de la Universidad, la realización de una actividad investigadora o la prestación de un servicio que conlleve el tratamiento de datos personales de los que dicha empresa, entidad u organización sea responsable.

Por ejemplo, puede ocurrir en contratos de investigación o prestación de servicios formalizados a través de la OTRI o servicio equivalente en el que un tercero subcontrate a la Universidad.

En este caso, también deberá firmarse el correspondiente contrato o acto jurídico de Encargo de tratamiento**.**
(Ver Anexo 1 - Cláusulas de encargo de tratamiento de datos personales)

6 ¿Puede el encargado del tratamiento recurrir, a su vez, a otro encargado (Sub encargado)?

El Encargado del tratamiento no podrá recurrir a un tercero para la ejecución total o parcial de los tratamientos de datos personales que tenga encomendados sin la autorización previa por escrito, específica o general, del Responsable del tratamiento.

Si la autorización es general, el Encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros Encargados, dando la oportunidad al Responsable de oponerse a dichos cambios.

Se recomienda incluir en el contrato o acto jurídico de Encargo de tratamiento una autorización específica que determine las entidades que van a ser subcontratadas, así como sus responsabilidades.
Estas también ostentan la condición de Encargado del tratamiento.

6.1 ¿Qué ocurre si es el subencargado quien incumple sus obligaciones en materia de protección de datos?

El subencargado también tendrá la condición de Encargado del tratamiento, por lo que será responsable de sus incumplimientos frente al Responsable y frente a los interesados. Sin perjuicio de

lo cual, en caso de incumplimiento por el subencargado, el Encargado inicial seguirá siendo plenamente responsable ante el Responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

7 ¿Qué ocurre si el objeto del servicio comporta el tratamiento de datos personales, pero es el prestador del servicio quién determina el alcance y los medios para el tratamiento?

Existen situaciones en las cuales la Universidad, pese a ser quién contrata el servicio, no establece el alcance y los medios a utilizar por parte del prestador del servicio. Habitualmente son servicios que se contratan por obligación legal, y la propia legislación que exige su contratación regula las actuaciones a realizar.

> Por ejemplo, la contratación de auditorías contables, en las cuales la empresa auditora tiene la potestad de decidir qué expedientes examina y cuáles no; la contratación de servicios de vigilancia de la salud, en los que existe un marco regulatorio que establece el nivel de información que el adjudicatario (la empresa especializada en salud laboral) debe hacer llegar al contratista (la universidad); etc.

En estas situaciones debe entenderse que cada parte (la universidad por un lado y el adjudicatario por otro) es Responsable del Tratamiento de los tratamientos de datos que realice, y en su caso habrá comunicaciones de datos entre responsables para permitir la consecución del objeto del contrato.

> Por ejemplo, la realización de los exámenes de la salud de los trabajadores y las trabajadoras de la Universidad implicará una comunicación de datos personales por parte de ésta a la empresa adjudicataria, con el fin de poder planificar las visitas. Una vez recibidos los datos, la adjudicataria tratará los mismos en calidad de Responsable del tratamiento.

Aunque no deba ser considerada Responsable de los tratamientos que realice la empresa adjudicataria, la Universidad debe garantizar que tanto los datos que le sean comunicados (si fuera el caso) como aquellos que la empresa pueda generar por motivo de la prestación del servicio, serán

tratados de acuerdo con la legislación vigente.

Así pues, será conveniente incluir en el contrato de prestación de servicios unas cláusulas que especifiquen claramente que cada parte es Responsable del Tratamiento de los tratamientos de datos que vaya a realizar y de las condiciones de cualquier comunicación de datos entre las partes, en caso de producirse**.**

8 ¿Qué ocurre si el objeto del servicio no comporta el tratamiento de datos personales, pero existe un riesgo de acceso a los mismos?

Recordemos que existe un encargo de tratamiento cuando una entidad (Responsable del Tratamiento) acuerda con otra (Encargado del Tratamiento) la prestación de un servicio por el cuál es necesario que el Encargado trate datos personales. Así pues, si la prestación del servicio no comporta el tratamiento de datos personales no podemos decir que exista un encargo de tratamiento.

No obstante, la prestación de determinados servicios puede suponer una posibilidad de acceso a datos personales por parte del proveedor.

Ejemplo: la contratación del desarrollo de una aplicación que, para su finalidad, precise gestionar alguna base de datos personales, si se desarrollase a partir de una base de datos de prueba previamente anonimizada; la contratación de servicios de limpieza de edificios; mudanzas; etc.

La inexistencia de un encargo de tratamiento no exime al Responsable del tratamiento de tomar unas precauciones mínimas **(artículo. 5.1.f RGPD)** con el fin de garantizar una protección contra el tratamiento no autorizado o ilícito, su pérdida, destrucción o daño accidental, mediante medidas técnicas u organizativas adecuadas.

En este caso, no será preciso formalizar un encargo de tratamiento. Pero, si existe el riesgo incidental

de acceso a datos personales, será conveniente tomar unas precauciones mínimas:

1) Por un lado, adoptar las medidas técnicas u organizativas adecuadas para garantizar una protección contra el tratamiento no autorizado o ilícito, la pérdida, destrucción o daño incidental de datos.
2) Además, será conveniente incluir en el contrato de prestación de servicios, cláusulas relativas al acceso incidental a datos personales, precisando las obligaciones y deberes de diligencia que en ese caso deberá adoptar el prestador del servicio.

Así pues, será conveniente incluir en el contrato de prestación de servicios unas cláusulas de acceso incidental a datos personales, las cuales serán distintas de las de Encargo de tratamiento y protegerán al Responsable en caso de mala conducta o negligencia por parte del prestador del servicio.

(***Ver Anexo 2 - Cláusulas de contratación de un servicio en el cual existe posibilidad acceso incidental a datos personales por parte del prestador) .***

9 ¿Pueden exigirse responsabilidades al encargado en caso de incumplimiento del encargo de tratamiento?

El Encargado de tratamiento responderá de sus incumplimientos en materia de protección de datos personales frente al Responsable del tratamiento y los interesados; sin perjuicio de que estos, puedan ejercitar sus derechos directamente frente al Responsable del tratamiento.

10 ¿Qué consecuencias tiene el incumplimiento de las obligaciones que el RGPD impone en materia de encargo de tratamiento de datos personales?

Para garantizar el adecuado cumplimiento de la normativa de protección de datos en toda la Unión Europea, el RGPD encomienda a las autoridades de control de todos los Estados miembros el ejercicio de "funciones y poderes efectivos, incluidos poderes de investigación, correctivos y sancionadores. Conforme a este mandato, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos

personales y garantía de los derechos digitales (a partir de ahora, LOPDGDD), desarrolla en su Título IX, el "Régimen sancionador" al que están sujetos, entre otros, los responsables de los tratamientos y los encargados de los tratamientos, establecido en el RGPD.

Para ello, la Ley Orgánica clasifica las infracciones en materia de protección de datos en muy graves, graves y leves (artículos 71 y siguientes de la LOPDGDD). Asimismo, establece los criterios para imponer las sanciones y medidas correctivas previstas en los apartados 4, 5 y 6 del artículo 83 del RGPD.

10.1 Infracciones en materia de Encargo de tratamiento

Específicamente, en materia de Encargo de tratamiento, se consideran **infracciones graves** **(artículo 73 LOPDGDD):**

J) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.

K) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del RGPD.

L) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

M) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

10.2 Consecuencias de una infracción por una Universidad privada

En caso de que la infractora sea una Universidad privada, la autoridad de control podrá imponerle como sanción una **multa administrativa,** que podría llegar **hasta los 20 millones de euros**, en función a las circunstancias del caso concreto **(artículo 76.1 y 2 LOPDGDD).**

De forma complementaria o alternativa a la imposición de una multa administrativa, será posible la adopción de las restantes **medidas correctivas** contempladas en el **artículo 83.2 del RGPD (artículo 76.3 LOPDGDD).**

Además, se publicará en el **Boletín Oficial del Estado** la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la **Agencia Española de Protección de Datos**, si la sanción fuese **superior a un millón de euros** y el infractor una **persona jurídica**.

En el caso de que la autoridad competente para imponer sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación **(artículo 76.4 LOPDDGDD)**; con el consiguiente **coste reputacional.**

Y, todo ello, sin perjuicio de las **responsabilidades penales y, en su caso, civiles, que las personas afectadas puedan exigir ante los tribunales ordinarios.**

10.3 Especialidades en el caso de infracción por una Universidad pública

En el caso de determinadas categorías de Responsables o Encargados de tratamiento, dentro de los cuales se incluyen las Universidades públicas, la comisión de una infracción en materia de protección de datos no conllevará la imposición de una infracción. En este caso, la autoridad de protección de datos competente dictará resolución sancionando a la Universidad con **apercibimiento** y estableciendo las **medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción** que se hubiese cometido.
La resolución se notificará al Responsable o Encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso **(artículo 77.2 LOPDGDD).**
Además, la autoridad de protección de protección de datos propondrá la **iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello.** En ese caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las **infracciones sean imputables a autoridades y directivos**, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una **amonestación** con denominación del cargo responsable y se ordenará la **publicación** en el Boletín Oficial del Estado o autonómico que correspondan **(artículo 77.3 LOPDGDD).**
Y, todo ello, sin perjuicio de las **responsabilidades penales y, en su caso, civiles** (por los daños y perjuicios materiales y morales que el incumplimiento haya podido causar), que las personas afectadas puedan exigir ante los tribunales ordinarios.
Por otro lado, la no inclusión del encargo de tratamiento o de las menciones mínimas del mismo legalmente exigidas, en los pliegos de cláusulas administrativas particulares de los contratos celebrados por las Universidades públicas, será causa de **nulidad de pleno derecho de los contratos celebrados**, de conformidad con la normativa vigente en materia de contratación pública. **(artículos 39 y 122 Ley Contratos Sector Público)**
En conclusión, aun no existiendo una multa económica, la apertura de un procedimiento sancionador frente a una Universidad por infracción en materia de protección de datos podrá entrañar un coste muy elevado para su reputación y daños y perjuicios para las personas afectadas. Por todo ello, es fundamental cumplir las obligaciones previstas y evitar incumplimientos.

Ejemplo de derecho comparado: Sanción a una Universidad italiana con 200.000 euros por deficiencias en su software de control de exámenes.

[…]

Aunque, el objetivo que perseguía la universidad con el uso de este software era el de intentar garantizar las mismas condiciones para aquellas personas que realizaban el examen, tanto de manera online como presencial, la universidad contrató un software conocido como Respondus, el cual en su calidad de encargado de tratamiento tiene su sede en Estados Unidos.

[…]

Así, entre las acciones que se llevaba a cabo con este software se encontraban la de grabar las pantallas de los estudiantes en distintos momentos durante las pruebas, llegando a detectar momento que pudieran ser considerados como sospechosos por los estudiantes, por ejemplo, cuando los estudiantes intentaban salir de la aplicación. Además, según se observó, el software también era capaz de detectar las caras de los estudiantes, por lo también en el tratamiento de datos biométricos.

Fuente: *(Ver:* https://www.legalarmy.net/sancion-a-una-universidad-italiana-con-200- 000-euros-por-deficiencias-en-su-software-de-control-de-examenes/)

11 Anexos

Anexo 1 – Cláusulas de encargo de tratamiento de datos personales.
Anexo 2 - Cláusulas de contratación de un servicio en el cual existe posibilidad acceso incidental a datos personales por parte del prestador.

Infografía para la contratación con terceros que implique tratamiento de datos.