Guía práctica para la Gestión de Riesgos de Terceros en Privacidad

www.ismsforum.es

dpi DATA PRIVACY INSTITUTE

isms forum

Copyright

Todos los derechos reservados. Puede descargar, almacenar, utilizar o imprimir la presente Guía práctica para la gestión de terceros en privacidad de ISMS Forum, atendiendo a las siguientes condiciones: (a) la guía no puede ser utilizada con fines comerciales; (b) en ningún caso la guía puede ser modificada o alterada en ninguna de sus partes; (c) la guía no puede ser publicada sin consentimiento; y (d) el copyright no puede ser eliminado del mismo.

GUÍA PRÁCTICA PARA LA GESTIÓN DE RIESGOS DE TERCEROS EN PRIVACIDAD

Con la participación de los siguientes profesionales y organizaciones:

Coordinación:

Adolfo Merino
Alfonso Javier Menchén
Carlos Alberto Saiz
Noelia Nogales

Colaboradores:

Araceli Fernández
Berta Balanzategui
Carlos Díaz
César Arquero
Cristina Sánchez-Tembleque
Elena Mora
Enrique Peloche
Francisco Rodríguez
Francisco Torres
Henry Velasquez
Javier Lomas
Jose María Cortés
Josep Bardallo
Leire Dúo
María Victoria Lacorzana
Mónica Garrido
Óscar Sánchez
Patricia Chenlo
Patricia Muleiro
Rosana Viejo
Susana Galiano
Susana Rey

Editor:

Daniel García, Director General de ISMS Forum

Diseño y maquetación:

Raquel García, Responsable de Comunicación Externa de ISMS Forum

ÍNDICE


SECURITY
REGULATIONS
INSPECTION
IN COMPLIANCE
IN COMPLIANCE
APPROVAL

ÍNDICE

ÍNDICE

01

Introducción y contexto actual

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, directamente aplicable desde el 25 de mayo de 2018, 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), ha supuesto un cambio total de paradigma a la hora de determinar y regular el cumplimiento de las obligaciones en materia de protección de datos, estableciendo la obligación legal para las empresas de adoptar un enfoque de riesgos frente a los viejos modelos de cumplimiento meramente formal.

El art. 5.2. RGPD recoge el principio básico de la "responsabilidad proactiva" o "accountabilty", tradicionalmente conocido también como "obligación de diligencia debida"; indicando que "El responsable del tratamiento será responsable del cumplimiento (…) y capaz de demostrarlo". Ello va a obligar a las empresas a que sean ellas mismas quienes determinen y evalúen cuáles van a ser las mejores medidas que les permitan cumplir con la normativa y poder demostrarlo, así como verificar periódicamente dicho sistema o medidas implantadas (art. 24.1. o 32.1.d RGPD).

En este contexto, donde además cada vez resulta mayor la dependencia de las empresas de sus proveedores y de la cadena de suministro, el deber de diligencia de las empresas no solo va a suponer un mayor conocimiento de la cadena de suministro y una mejora en la toma de decisiones, sino que además esa diligencia debida constituye una obligación legal impuesta por la normativa de protección de datos pero también otro tipo de normativas, como por ejemplo la penal, o normativas sectoriales específicas (banca, seguros, telecomunicaciones, infraestructuras críticas, etc.), que obliga a las empresas a contar con "compliance programs", a tener políticas de externalización de servicios y evaluación de proveedores, a analizar y evaluar los riesgos, controlar y supervisar a los proveedores que accedan a datos personales a lo largo de todo el ciclo de vida de la propia prestación de servicios que realicen (elección del proveedor, negociación y firma de contrato, monitorización y vigilancia del cumplimiento del contrato, terminación de la prestación de servicios, etc.) e incluso a determinar conjuntamente con los proveedores los controles de los riesgos.

El objeto de la presente guía, establecer unas pautas generales, recomendaciones o buenas prácticas que permitan a las empresas concretar e implementar ese principio general de la diligencia debida, especialmente a la hora de elegir a sus proveedores. Tras definir en los capítulos 1 y 2 las obligaciones legales existentes, el capítulo 3 se centra en concretar cuáles son esas buenas prácticas según la fase en la que vaya teniendo intervención el proveedor: fase pre-contractual, fase contractual y fase de terminación de la relación contractual.

02

Regulación de la obligación de la diligencia debida

2. Regulación de la obligación de la diligencia debida

El art. 24. 1.RGPD exige que el responsable aplique medidas técnicas y organizativas apropiadas y que las revise y actualice cuando sea necesario, y en el art. 28.1 le indica al responsable que elegirá un proveedor/encargado que pueda aplicar medidas técnicas y organizativas suficientes.

El Considerando 81 RGPD resulta sumamente esclarecedor al señalar que el responsable (…) debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento (…).

Dado que cada vez el entorno legislativo en la que una empresa pública o privada desarrolla su actividad es cada vez más profuso y el impacto de incumplimiento de regulación es más intenso que nunca, se hace necesario que las empresas elaboren sus propios "compliance programs" no solo para garantizar el cumplimiento de las obligaciones legales, sino para mejorar sus medidas internas de control, obtener una mayor reputación en el mercado, evitar el fraude interno así como también sanciones administrativas y/o judiciales.

De ahí, la gran importancia de que las empresas cuenten con esos sistemas o marcos de control que les permita también conocer, elegir, contratar, y controlar a los proveedores en materia de privacidad y ello con carácter previo a la puesta en marcha del correspondiente tratamiento o prestación del servicio.
adecuada realización de auditorías RGPD.

2.1. El Cumplimiento

A diferencia del régimen normativo anterior, basado exclusivamente en un cumplimiento meramente formal y/o contractual, el RGPD da un paso más en su enfoque de riesgos y exige una mayor responsabilidad y control a los responsables y encargados no solamente al momento contractual sino también a los momentos anteriores y posteriores a la firma del contrato, e incluso en el momento de la terminación de dicha relación o prestación de servicios.

Por eso, el responsable del tratamiento, de acuerdo con lo previsto en el art. 28 RGPD, va a ser responsable de que su proveedor/encargado del tratamiento (en los tratamientos que por cuenta del responsable realice) cumpla con el RGPD. En este sentido, Las "Directrices para la elaboración de contratos entre responsables y encargados de tratamiento" elaboradas por la AEPD, APDCAT y AVPD señalan que el RGPD establece una obligación de diligencia debida

en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD. Y ello, implica la necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.

La empresa, responsable del tratamiento, debe valorar, controlar y supervisar que su proveedor está utilizando y accediendo a datos personales, en los términos exigidos por el RGPD. Esa valoración de cumplimiento de los proveedores, encargados de tratamiento, deberá realizarse con carácter previo y anticipado a la puesta en marcha del correspondiente tratamiento o prestación de servicios por parte del proveedor y deberá comprender, entre otros, los siguientes análisis o tareas: (i) Que en el uso de la información personal se respetan los principios establecidos en el artículo 5 RGPD (ii) Que se han previsto y adoptado un conjunto de Medidas de seguridad, técnicas y organizativas (art. 32) (iii) Que dichas medidas de seguridad se van a verificar y revisar periódicamente (art. 24.1.) (iv) Que existen determinadas Políticas internas y procedimiento que permitan cumplir con la privacidad desde el diseño (art.25 RGPD) (v) Que cuenta con un Registro de Actividades de tratamiento, en los casos que resulte necesario (art. 30RGPD) (vi)Que cuentan, en los casos exigidos, con un Delegado de Protección de Datos (art. 37-39 RGPD) (vii) Que se van a notificar y/o comunicar las de Brechas de seguridad que, en su caso, pudieran producirse (art. 33 y 34 RGPD) (viii) Que se han llevado a cabo los pertinentes análisis de riesgos y/o evaluaciones de impacto (art. 35 RGPD) (ix) Que se realizan o no Transferencias internacionales de datos (art. 44 RGPD).

2.2. La prueba del Cumplimiento

Ahora bien, esa actuación diligente a la hora de elegir proveedor/encargado de tratamiento no puede quedar solamente en la valoración del cumplimiento expuesta en el anterior apartado, sino que además el responsable del tratamiento, y por extensión el propio encargado o subencargado, deben demostrar y acreditar que efectivamente cumplen con la normativa aplicable.

Es decir, no basta únicamente con firmar un contrato en las que se especifique que se cumple con lo establecido en el artículo 28 de RGPD, sino que, para cumplir con el principio de responsabilidad proactiva, es necesario demostrar que los intervinientes tienen implementada una fuerte "cultura de cumplimiento" y que sus "compliance programs" son efectivos y que tienen establecidos procedimientos de control y supervisión.

En este sentido, a fin de poder demostrar cumplimiento, el propio RGPD nos da algunas pautas o indicaciones, de lo que en determinados ámbitos resulta obligatorio tanto para responsables como para encargados, a saber: a) Adopción e implantación de determinadas medidas como: seudonimización, minimización/reducción de tratamientos, transparencia, supervisión

de tratamientos, promoción de desarrollo y fabricación de productos con una privacidad por defecto, etc. (C. 78 RGPD). b) Revisión y actualización de medidas o controles que garanticen la seguridad del tratamiento (C.81 y art. 24.1 RGPD), previamente determinados y/o exigido al proveedor c) Contar con un Registro de actividades de tratamiento (C. 82) d) Adoptar las garantías adecuadas en los casos de estar ante una transferencia internacional de datos (decisión de la comisión, cláusulas contractuales tipo, etc. (C.108)

En este sentido, los considerandos 81,108, 109 y 110 RGPD hacen referencia expresa a determinados elementos que, en su caso, podrían servir para demostrar el cumplimiento de obligaciones o facilitar la labor de prueba de responsables y encargados del tratamiento.

Así, podemos concluir con algunas medidas generales de "diligencia debida" que los responsables están obligados a adoptar y que la propia Agencia Española de Protección de Datos definió en la "Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento"

2.3. Consecuencias del incumplimiento de la obligación de diligencia debida

Sin ánimo de exhaustividad, el incumplimiento de la obligación de diligencia debida y, por tanto, la ausencia de control en materia de privacidad en la elección de un proveedor, podría dar lugar a diferentes tipos de responsabilidad:

Responsabilidad penal

Tanto el responsable del tratamiento como la empresa proveedora de servicios, con independencia de la relación y responsabilidades contractuales, deberán prestar especial atención al riesgo de comisión de un delito de descubrimiento o revelación de secretos (apoderamiento o interceptación de mensajes de correo electrónico, interceptación de comunicaciones, utilización o modificación de información personal o familiar para vulnerar la intimidad) o de daños informáticos (que regula todo tipo de intromisiones en plataformas ajenas o sistemas externos como: destrucción -total o parcial- o alteración -eliminación, interrupción, supresión o borrado- de datos, programas o elementos informáticos); ante la falta de controles a la hora de elegir o contratar con dicho proveedor. A modo de ejemplo, se prevé una modalidad agravada de este último delito, en el caso de que se afecte a los sistemas informáticos de una infraestructura crítica, y que lógicamente podría afectar a aquellos proveedores de dicha infraestructura crítica.

En este sentido, cobran especial relevancia los "Compliance Programs", y los sistemas de control de proveedores que incluyan; ya que el responsable o el proveedor podrían quedar exen-

tas de una posible e hipotética responsabilidad penal siempre que cuenten, según los art. 31 bis.2 y 31 bis.5 CP, con un programa real y efectivo de "Compliance" y de prevención de delitos.

Responsabilidad administrativa

El artículo 83 (5) (a) del RGPD establece que las infracciones de los principios básicos para el procesamiento de datos personales, entre los que se encuentra el de la diligencia debida o responsabilidad proactiva, podría suponer una multa de hasta 20 millones de euros, o el 4% de su facturación anual mundial total, optándose por la que sea mayor.

En el mismo sentido, la LOPD señala que las infracciones tanto al RGPD como a la propia LOPDGDD (art. 70-78), podrán ser muy graves, graves o leves y ser sancionadas con las multas previstas en el RGPD.

La Ley 34/2002, de 11 de julio de servicios de la sociedad de la información y de comercio electrónico, establece que el incumplimiento de las obligaciones señaladas en la propia norma y en particular la referida a la prohibición de comunicaciones comerciales por correo electrónico o medios equivalentes, podría determinar la entrada en juego del régimen sancionador de la propia norma que oscilaría entre multas de 0€-600.000€, según estemos ante una infracción leve, grave o muy grave.

Por su parte, también debe tenerse en cuenta el régimen sancionador de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones ya que el incumplimiento de las obligaciones señaladas en la propia norma y en particular las derivadas de la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, datos de tráfico y localización, ex. Art.48,

Responsabilidad civil

La responsabilidad civil se puede definir como la obligación de pagar por los daños y perjuicios causados a una persona o empresa y a su patrimonio, como consecuencia del incumplimiento de un contrato (artículo 1101 del Código Civil -quedan sujetos a la indemnización de los datos y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tener de aquéllas-) o aunque no exista vínculo contractual alguno (artículo 1902 CC- El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado).

03

Responsabilidades de cada figura

Tanto el responsable del tratamiento como los corresponsables y los encargados y subencargados desempeñan diferentes roles teniendo una serie de obligaciones legales que describiremos a continuación. Así, según los art. 24, 25 y 28.1. y 2. RGPD, los responsables deberán aplicar, implementar, monitorizar, controlar, revisar y actualizar las correspondientes medidas técnicas y organizativas que garanticen un tratamiento de la información personal adecuada al RGPD, y en su caso, elegir un proveedor que cumpla y garantice dichas medidas técnicas y organizativas. Por lo tanto, el responsable deberá establecer un sistema de control del propio proveedor, con anterioridad a la elección y contratación de mismo para conocer si puede ofrecernos o no medidas técnicas y organizativas adecuadas, como podría ser el tener un procedimiento de homologación de proveedores. Uno de los grandes cambios del RGPD ha sido el establecer obligaciones separadas e independientes tanto para responsables como para encargados, tal y como veremos en los apartados siguientes.

Antes de entrar a exponer las concretas obligaciones que debe cumplir cada figura, se hace necesario advertir la importancia de analizar desde el inicio si el servicio que se quiere externalizar conlleva el acceso de datos de carácter personal de un tercero y de establecer los roles y las responsabilidades de cada uno. De este modo ambas empresas podrán garantizar que cumple con la normativa de protección de datos y definir correctamente las obligaciones de cada uno de ellos y definir si realmente existe un encargo de tratamiento o si por el contrario nos encontramos ante otras figuras jurídicas como por ejemplo (corresponsables o acuerdos de colaboración que suponga una cesión de datos).

Por tanto, desde la fase inicial hay que definir: (i) quién determina los fines del tratamiento y la manera en que se procesa los datos de carácter personal (ii) quien recopila los datos y determina la base legitimadora del tratamiento (iii) quién determina los fines del tratamiento (iv) sobre quién individuos se recopilan los datos (v) por cuánto tiempo se deben conservar los datos. Una vez analizado el rol que desempeña cada uno de los intervinientes en la relación contractual que se pretende formalizar, podremos definir las obligaciones de cada uno.

3.1. El Responsable del Tratamiento

Los responsables asumen el nivel más alto nivel de responsabilidad: deben cumplir y demostrar el cumplimiento del RGPD y también son responsables del cumplimiento de su proveedor/encargado. De acuerdo con el art. 4.7) RGPD el responsable es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros,

determine los fines y medios del tratamiento".

Es decir, que son aquellos que toman decisiones sobre las actividades de uso o tratamiento de la información personal. Ejercen un control general de los datos personales que se tratan y, en última instancia, están a cargo y son responsables de dicho tratamiento.

Sus principales obligaciones son:

Cumplir con los principios de protección de datos.	Notificación a la autoridad de control y/o a los interesados de las brechas de seguridad.
Velar por que los ciudadanos puedan ejercitar sus derechos.	Cumplir con obligaciones específicas (registro actividades, elaboración de PIAS, nombramiento DPO...)
Implementar medidas de seguridad técnicas y organizativas para garantizar la seguridad de los datos.	Cumplir con los requisitos legales cuando se realice una Transferencia Internacional de Datos.
Formalización contrato conforme artículo 28.	Nombramiento de un representante dentro de la Unión Europea.
Cooperar con la autoridad de control.	

Además, el responsable está obligado a elegir un proveedor/encargado que cumpla y pueda demostrar que cumple y que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD. Esta obligación también se extiende a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

3.2. Los Co-Responsables del Tratamiento

La corresponsabilidad es una figura nueva en el marco legal español que introduce el Reglamento General de protección de datos en su artículo 26 y que se define como: *Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento*.

Ha de tenerse en cuenta que para que exista la corresponsabilidad es necesario que, total o parcialmente, sean de forma conjunta e igualitaria todos los intervinientes los que tomen las decisiones relacionadas con la finalidad, incluso si para cada uno esta fuese diferente se decidirá conjuntamente, y los medios a utilizar, tecnológicos, humanos, procedimientos, proveedores, etc.

La corresponsabilidad no es para nada un Encargo del Tratamiento, en el que las decisiones las toma únicamente el Responsable y el Encargado únicamente ejecuta acciones en base a las instrucciones de este. Pero tampoco se corresponde con una relación en la que, dentro de un determinado proceso de tratamiento de datos, una parte ejerce como Responsable único en parte del proceso, y otra u otras en otras partes del mismo. Es necesario esa determinación conjunta de fines y medios en todas las fases del tratamiento. En base a toda la definición previa vemos que la relación de corresponsabilidad se establece siempre en el marco de un Tratamiento concreto, no en una relación mercantil en su conjunto. Puede darse el caso en que dos empresas sean Corresponsables para ciertos Tratamientos y Responsable-Encargado para otros.

Un **ejemplo** de corresponsabilidad muy claro y que se recoge en el artículo 20 de la LOPDyGDD es el de los *sistemas de información crediticia*. Un ejemplo en el que hay dos Responsables y sin embargo no existe corresponsabilidad se dará, por ejemplo, en la relación entre una empresa de marketing dedicada a la *captación de leads* en Internet, que posteriormente vende esta información a una empresa interesada en utilizarlos para realizarles comunicaciones comerciales.

Los Corresponsables tienen cada uno de ellos las mismas y todas las obligaciones que la legislación fija para un Responsable. Pero además, en el mismo artículo 26 y en el artículo 29 de la LOPDyGDD se añaden una serie de Obligaciones a cumplir para este tipo de relación:

Establecimiento de un contrato en el que se fijen para cada una de las obligaciones legales correspondientes a un Responsable del Tratamiento, vistas en el apartado anterior, que asumirá cada parte.	El contrato debe fijar al menos la responsabilidad en cuanto al deber de información al interesado y al ejercicio de derechos.

Gestionar los derechos de los interesados independientemente de ante que sociedad se presenten y aunque no sea esta la contemplada en el contrato.	Publicación del acuerdo o al menos de las partes que afecten a los interesados.

3.3. El Encargado del tratamiento

De acuerdo con el art. 4.8) RGPD el encargado es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

Los encargados actúan en nombre y por cuenta del responsable y siguiendo sus indicaciones y sirviendo o prestando servicios al responsable. Ello no significa que el encargado no pueda tomar sus propias decisiones operativas, pero siempre dentro del marco y de acuerdo con las instrucciones dadas por el responsable.

Las obligaciones del encargado no se circunscriben al estricto ámbito del contrato que los une con el responsable; sino que el propio RGPD establece obligaciones concretas y diferenciadas para dichos proveedores/ encargados de tratamiento, y que además podrán ser supervisadas separadamente por las autoridades de protección de datos:

Tratar los datos siguiendo las instrucciones del responsable.	Notificar al responsable ante cualquier incumplimiento de RGPD u otras normativas de protección de datos que pudieran estar produciendo sus instrucciones.
Celebración de un contrato conforme artículo 28 RGPD.	Cumplir con las obligaciones específicas que señala el propio (registro de actividades, nombramiento de un Delegado de Protección de Datos, en los casos exigidos por el RGPD).

Prohibición de contratar a otro encargado sin la autorización previa del responsable, debiendo celebrar un contrato de subencargado en los mismos términos o equivalentes al celebrado con el responsable.	Velar porque cualquier transferencia de datos personales fuera del EEE esté autorizada por el responsable del tratamiento y cumpla con los requisitos del RGPD (mismo nivel de protección, garantías adecuados, decisiones marco de la comisión, normas corporativas vinculantes, cláusulas contractuales tipo).
Implementar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, disponibilidad e integridad de los datos personales.	Nombramiento de un representante dentro de la Unión Europea.
Notificar sin demora alguna las Brechas de datos personales, a fin de que el responsable pueda cumplir en tiempo y forma sus obligaciones de notificación al regulador.	Nombramiento de un representante dentro de la Unión Europea.

Para demostrar que ofrecen las garantías exigidas por el RGPD, los encargados podrán adherirse a códigos de conducta, certificarse dentro de los esquemas previstos por el RGPD o facilitar mecanismos de realización de auditorías

3.4. Los subencargados del tratamiento

Según lo establecido en el art. 28.4. RGPD, cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

Por tanto, ese otro encargo al que se refiere el RGDP no es otra cosa que el subencar-

gado que tendrá las mismas obligaciones y responsabilidades frente a su encargado que las que este tiene frente al responsable del tratamiento. Y ello, sin perjuicio de la obligación del encargado ex art. 28.2.RGPD de informar al responsable acerca de los concretos subencargadados del tratamiento.

Las obligaciones del subencargado no se circunscriben al estricto ámbito del contrato que los une con el encargado; sino que el propio RGPD establece las mismas obligaciones concretas y diferenciadas que establece para los encargados del tratamiento, y que además podrán ser supervisadas separadamente por las autoridades de protección de datos:

Tratar los datos siguiendo las instrucciones del encargado/ responsable.	Notificar al encargado ante cualquier incumplimiento de RGPD u otras normativas de protección de datos que pudieran estar produciendo sus instrucciones.
Celebración de un contrato conforme artículo 28 RGPD.	Cumplir con las obligaciones específicas que señala el propio (registro de actividades, nombramiento de un Delegado de Protección de Datos, en los casos exigidos por el RGPD).
Prohibición de contratar a otro subencargado sin la autorización previa del encargado/ responsable, debiendo celebrar un contrato de subencargado en los mismos términos o equivalentes al celebrado con el encargado/responsable.	Velar porque cualquier transferencia de datos personales fuera del EEE esté autorizada por el encargado/ responsable del tratamiento y cumpla con los requisitos del RGPD (mismo nivel de protección, garantías adecuados, decisiones marco de la comisión, normas corporativas vinculantes, cláusulas contractuales tipo).
Implementar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, disponibilidad e integridad de los datos personales.	Nombramiento de un representante dentro de la Unión Europea.

Notificar sin demora alguna las Brechas de datos personales, a fin de que el encargado/ responsable puedan cumplir en tiempo y forma sus obligaciones de notificación al regulador.	Cooperación con las autoridades de supervisión y control.

Para demostrar que ofrecen las garantías exigidas por el RGPD, los subencargados podrán adherirse a códigos de conducta, certificarse dentro de los esquemas previstos por el RGPD o facilitar mecanismos de realización de auditorías

En cuanto a los responsables del tratamiento, además de seguir ostentando su principal papel a la hora de determinar los medios y fines del tratamiento, así como todas las obligaciones indicadas en el apartado 2.2., cobra especial relevancia la obligación de autorizar de manera previa y por escrito (bien de manera general bien de manera específica) la subcontratación realizada por el encargado del tratamiento, así como controlar y vigilar los cambios en dichas autorizaciones.

Por su parte, el encargado del tratamiento, además de las mismas obligaciones indicadas en el apartado 2.2., debe facilitar al responsable el listado de subencargados para facilitar la autorización por parte del responsable, así como hacer mención al contrato existente entre dichos subencargados y el encargado. Igualmente, el encargado deberá exigir a los subencargados las mimas obligaciones y garantías que él tiene en su contrato frente al responsable, siendo responsable del cumplimiento de las obligaciones del subencargado frente al responsable del tratamiento.

04

Fase Precontractual

4.1. Introducción

Tal y como anticipamos en el Capítulo 1 de la presente Guía, en el **artículo 28 del RGPD** se establece la obligación de elegir únicamente a aquellos encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de tal manera que el tratamiento que realicen por cuenta del responsable sea conforme con los requisitos establecidos en la citada normativa.

En este mismo sentido se pronuncia el legislador europeo en el considerando 81 del Reglamento, donde establece que las garantías que debe ofrecer el encargado están relacionadas con los conocimientos especializados que tenga en la actividad de tratamiento que vaya a llevar a cabo en nombre del responsable, su fiabilidad en cuanto a la realización del tratamiento y los recursos con los que debe contar para aplicar medidas técnicas y organizativas adecuadas al tratamiento de datos que vaya a realizar.

De lo anterior se desprenden dos cuestiones a tener en consideración; por un lado, que los responsables del tratamiento deben ser diligentes a la hora de elegir a sus encargados y; por otro, que los encargados del tratamiento, con carácter previo a su contratación, tienen que ofrecer a los responsables las garantías que resulten adecuadas al nivel de riesgo identificado, facilitando las evidencias que permitan acreditar el cumplimiento de estas.

En cuanto a lo anterior, el considerando del Reglamento, establece que la adhesión del encargado a un código de conducta o a un mecanismo de certificación aprobados por las autoridades de control competentes puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable.

No obstante, en la actualidad, ni las autoridades de control competentes ni el Comité Europeo de Protección de Datos, han desarrollado los esquemas de certificación o aprobados suficientes códigos de conducta, para que las garantías enunciadas puedan ser aplicadas o tenidas en consideración por los responsables a la hora de seleccionar a sus encargados.

Entre tanto o como refuerzo de las citadas garantías y de conformidad con el principio de responsabilidad proactiva, los responsables deben implementar mecanismos y criterios que les permitan seleccionar a los encargados, así como evidenciar ese deber de diligencia frente a las autoridades de control competentes.

Entre los mecanismos que los responsables pueden implementar en sus organizaciones con dicho propósito, están, además de los reconocidos expresamente en el Reglamento, la adopción de criterios de evaluación y selección de proveedores que permitan analizar la capacidad de éstos de ofrecer garantías suficientes, para aplicar las medidas que resulten necesarias durante el tratamiento de los datos.

En este sentido, los responsables podrán optar, bien por desarrollar e implementar políticas y procesos internos que les permitan llevar a cabo la evaluación y selección de proveedores de manera objetiva y evidenciable, o bien, contratar los servicios de un tercero de confianza que haya desarrollado unos criterios de evaluación propios que permita a los responsables seleccionar a sus proveedores basándose en la información facilitada por dicho tercero.

En cuanto a la primera opción, es necesario que las políticas y procedimientos internos sean conocidas por todas las personas que participen en el proceso de selección, incluidas las unidades contratantes, siendo imprescindible la formación y concienciación continua de dichas personas sobre la materia. Del mismo modo, será necesario establecer una supervisión y control efectivos del cumplimiento de todo el proceso, verificando periódicamente la eficacia de los controles implementados en el mismo.

En este sentido, resulta recomendable que los criterios establecidos por el responsable para la selección de encargados del tratamiento, por ejemplo, en el momento de publicar una licitación, sean conocidos con carácter previo por éstos, de cara a que los tengan en cuenta a la hora de realizar sus ofertas a los responsables o participar en las licitaciones publicadas por aquellos.

En relación con la segunda opción, es decir, que se acuda a los servicios de un tercero de confianza para la selección de proveedores, es necesario estar familiarizado con los criterios establecidos por dicho tercero para evaluar y clasificar a los proveedores y que los mismos se encuentren alineados con las exigencias del responsable. Asimismo, es conveniente demandar al tercero absoluta transparencia en relación con los servicios que presta y los mecanismos empleados en la evaluación y clasificación de los proveedores, así como su colaboración a la hora de evidenciar frente a las autoridades de control el deber de diligencia con el que ha de actuar el responsable en la selección de sus proveedores.

Dicho esto, a continuación, se desarrollarán algunas propuestas para la correcta clasificación y evaluación de encargados que permitan a los responsables seleccionar a

aquellos proveedores que ofrezcan garantías apropiadas, cumpliendo así los requisitos establecidos en la normativa de protección de datos.

4.2. El proceso de homologación

La complejidad de este proceso será mayor o menor dependiendo del tipo de responsable del tratamiento que nos encontremos, más sencillo cuando se trate de una pequeña empresa, dónde tanto el número de terceras partes colaboradoras así como la estructura interna de la compañía son más pequeñas, más complejo, a medida que el tamaño de la empresa y el número de terceras partes aumenten, lo que implicará un mayor esfuerzo en la tarea de implementar y "sincronizar" este proceso al resto de procedimientos internos.

Así, en grandes o medianas empresas dónde existen diferentes departamentos susceptibles de estar involucrados, desde el equipo legal y DPO, los profesionales de IT, y por supuesto los responsables de compras, será necesario definir con claridad los roles, responsabilidades y puntos de control que corresponden a cada parte participante en el proceso. La coordinación y estructuración del proceso de manera horizontal a todas las partes involucradas garantizará los mejores resultados en la selección de terceros.
Cuando se trate de pequeñas empresas, dónde la naturaleza y estructura de la compañía es más sencilla, el procedimiento podrá definirse involucrando a un menor número de personas de manera más rápida y sencilla, sin embargo, es importante que tenga el soporte necesario, ya sea a nivel interno en la empresa, o externo, a través de la contratación de servicios especializados, para garantizar la correcta evaluación y selección del proveedor.

En todo caso, se tratará siempre de asegurar el "principio de responsabilidad proactiva" del que ya hablamos en la introducción, además de minimizar de forma efectiva el riesgo de potenciales brechas de seguridad debido a una mala gestión del tratamiento de datos personales por parte de un tercero.

Como ya dijimos, el procedimiento deberá ser transversal a todas las unidades de negocio implicadas en la selección de proveedores, pero además debe tener la **capacidad o entidad suficiente para determinar si finalmente procede o no, iniciar la contratación** del mismo. Será también fundamental impartir una adecuada formación específica en la materia a los trabajadores involucrados, lo que además reforzará a modo de evidencia, que estamos cumpliendo con el principio de responsabilidad proactiva.

La protección de datos se convierte así, en otro elemento fundamental previo a la selección del proveedor, junto con las ya tradicionales cuestiones de negocio, financieras o logísticas. Aunque el procedimiento que nos ocupa es adaptable a las circunstancias y características de cada responsable, a continuación enumeramos los pasos o diferentes fases que, con independencia del tamaño o características del responsable, deben siempre tenerse en cuenta o incluirse:

4.2.1. Identificación y clasificación de terceros

Antes de llevar a cabo la evaluación, dónde pasaremos a examen de manera exhaustiva a cada uno de nuestros proveedores, es importante conocer el escenario ante el que nos encontramos, de manera que esto nos ayude a llevar a cabo una posterior evaluación exhaustiva y eficiente.

Lo siguiente pasos, a tener en cuenta cronológicamente, nos ayudaran a obtener el resultado deseado:

1. **Identificación de todos los proveedores que vayan a tratar datos personales por cuenta de nuestra organización:** En toda organización el primer paso debe comenzar por la detección o identificación de todos aquellos tratamientos susceptibles de ser llevados a cabo en nuestro nombre por terceros. Es esencial, para poder continuar con el procedimiento, ser exhaustivos en la detección de todos los potenciales tratamientos.

Para llevar a cabo esta tarea es recomendable apoyarse en el RAT (Registro de actividades del tratamiento), a su vez, y de manera inversa, tenemos la oportunidad de actualizar el propio RAT incluyendo los nuevos tratamientos detectados, lo que nos permitirá que el proceso esté en todo momento alineado con esta herramienta de cumplimiento normativo.

Será esencial en este primer paso, involucrar a los responsables de negocio y del procedimiento interno involucrado, ya que son ellos quienes mejor pueden proporcionaros información sobre la actividad detallada que realizará la tercera parte en cuestión y, por tanto, sobre el potencial tratamiento de datos que puede llevarse a cabo.

Otra cuestión importante de esta parte, será diferenciar de manera correcta, cuándo se trata de "encargos del tratamiento" y cuándo, por el contrario, se trata de "comunicaciones de datos" dónde las terceras partes adquieren el rol de responsables. Cuestión que en ocasiones genera disputas entre las empresas.

El resultado final, será por tanto un listado o clasificación, que nos permita conocer todos aquellos proveedores que acceden o tratan nuestros datos. Dicho listado, puede clasificarse además con base en las unidades de negocio de nuestra compañía o, por ejemplo, en los diferentes servicios que ofrecemos, en definitiva, incluyendo toda aquella información adicional y necesaria que nos permita en todo momento localizar de manera clara y eficiente el tratamiento y sus implicaciones en el negocio.

Tabla 1.1: *A continuación, mostramos un ejemplo del posible resultado tras esta primera parte, la tabla expuesta es solo un ejemplo que puede ser personalizada o adaptada atendiendo a las características de cada empresa, y a la información adicional que cada empresa decida incluir.*

.

Proveedor	¿Tratamiento de datos por nuestra cuenta?	Actividad del tratamiento (RAT)	Tipo de Servicio	Responsable del servicio	Tipología de los datos
SUPERMKT S.L	SI	Registro de clientes online	Ventas website	Alfredo Perez	Datos de contacto y bancarios de cliente final

2. Análisis respecto a la tipología de los datos que van a ser tratados. En el siguiente paso debemos profundizar sobre la tipología de los datos que van a ser tratados, así como del tipo de tratamiento que sobre ellos se realizará. Tomando como referencia la tabla anteriormente expuesta, se trata de desglosar la información contenida en la última columna lo que nos ayudará, además, a identificar el nivel de riesgo de cada proveedor, entendiendo riesgo como la probabilidad de producirse una brecha o incidente sobre un determinado tratamiento y el impacto que tendría no solo sobre el responsable, sino también sobre los titulares.

Uno de los puntos clave será determinar si nos encontramos ante tratamientos de datos sensibles, lo que supondrá un incremento del riesgo, de las medidas de seguridad necesarias y, por tanto, del nivel de exigencia en la posterior evaluación que llevaremos a cabo. Deberá atenderse también a si la naturaleza del tratamiento que se realizará implica especiales riesgos para el responsable respecto a la **confidencialidad, integridad y disponibilidad** de la información, lo que además, como ya dijimos, supondría de

forma inherente un riesgo para los titulares de los datos. Las empresas que cuenten con departamentos de seguridad de la información, IT, o CSOs, pueden incorporar a dichos profesionales al proceso de cara a mejorar el control y las medias de mitigaciones de los tratamientos que involucren especial riesgo para la compañía.

No obstante, el riesgo podrá medirse de manera generalizada utilizando parámetros similares a los utilizados en las evaluaciones de impacto o procedimientos de gestión de brechas de seguridad, especialmente atendiendo a la tipología de los datos involucrados, a su volumen, la capacidad de recuperarlos en caso de pérdida, etc.

Ejemplo: Otorgar acceso y compartir una base de datos de contactos profesionales con un tercero tendrá diferentes consecuencias y un nivel de riesgo menor para la compañía que, por ejemplo, poner en manos de terceros información relativa a la salud de empleados o clientes.

3. **Análisis de la situación contractual.** De cara a facilitar la labor de nuestro equipo legal, será recomendable añadir al listado o clasificación que venimos elaborando, la situación contractual en la que se encuentran los servicios bajo los cuales se llevará a cabo el tratamiento.

Las circunstancias podrán ser diversas, pero a continuación enumeramos algunas de las que pueden considerarse más habituales:

- Que ya exista un contrato con el proveedor, pero que no se haya recogido en un Acuerdo de Tratamiento de Datos (Art. 28) el tratamiento a llevar a cabo, bien porque anteriormente no se realizaba, o porque en su momento, especialmente en contrataciones antiguas cuando la protección de datos podía pasar desapercibida para algunas compañías, no se identificó correctamente. En ambos casos, deberá actualizarse la relación contractual incluyendo el mencionado acuerdo.

- Que no exista ningún tipo de contrato ya que el proveedor es nuevo. En tal caso, y con base en este proceso de homologación, deberá articularse el preceptivo acuerdo de tratamiento de datos.

- En un tercer supuesto, existe la posibilidad de que para el tratamiento en cuestión, exista un Acuerdo de tratamiento de datos con una tercera compañía la cuál dejará de llevarlo a cabo por finalización del servicio. Debemos en este caso de atender al clausulado del acuerdo para una correcta devolución o transfe-

rencia de los datos por parte del proveedor que finaliza el servicio.

4. Preparación de la evaluación y requisitos de cumplimiento normativo. En este punto, contando ya con la identificación y clasificación exhaustiva de cada proveedor, y su información relativa al tipo de tratamientos que llevará a cabo, es momento de darle forma a la evaluación que se llevará a cabo para verificar todos los puntos de cumplimiento normativo. En la letra a) del subapartado siguiente, se enuncian algunos de los criterios que se pueden tener en consideración a la hora de analizar el grado de cumplimiento de la normativa por parte del tercero que se está analizando.

Es necesario tener en cuenta que no hay un listado numerus clausus, por lo que la comprobación del cumplimiento de la normativa del encargado podrá llevarse a cabo de diferentes modos. Se podrá adaptar dicha evaluación, reforzando el componente técnico, cuando por ejemplo los tratamientos impliquen importantes medidas de seguridad (proveedores de ingeniería, servicios de Cloud), o poner el foco en la relación con clientes finales, clausulas informativas, comunicaciones comerciales en los casos en los que el tratamiento está relacionado con la gestión de datos de nuestros clientes. El trabajo realizado hasta ahora, nos permite adaptar el examen de manera detallada a cada tipo de proveedor. Sin embargo, no hay que olvidar que no todos los proveedores tendrán el mismo carácter de obligatoriedad para el cumplimiento de la normativa.

4.2.2. Evaluación de terceros

En cuanto a la evaluación de los proveedores, a continuación, se propone seguir el siguiente esquema:

a) Organización y gobernanza de la privacidad. El proceso de homologación ha de incluir la evaluación de la organización y gobernanza de la privacidad del proveedor, verificando y revisando la existencia de criterios relativos a protección de datos y otros aspectos del gobierno y cumplimiento de la normativa como, por ejemplo:

1. La posible adhesión a códigos de conducta.
2. La posesión de un certificado de protección de datos.
3. En su caso, el nombramiento de DPO y su registro ante la autoridad de control competente.
4. La realización o no de Transferencias Internacionales de Datos, y en tal caso la existencia de garantías adecuadas para llevarla a cabo de acuerdo con la regulación.

5. La llevanza de un Registro de Actividades de Tratamiento.
6. La implementación de políticas internas relativas al tratamiento de datos personales (ejercicios de derechos, comunicación de incidentes de seguridad, gestión de personal etc.).
7. La existencia de posibles subcontrataciones (subencargados del tratamiento y los correspondientes acuerdos de protección de datos con terceros).
8. La existencia de antiguas sanciones al encargado del tratamiento en materia de protección de datos.
9. La existencia de sentencias condenatorias y/o procedimientos judiciales abiertos en materia de protección de datos respecto del encargado del tratamiento.

Cada uno de los requisitos examinados deberá ir acompañado de los preceptivos comentarios por parte de la persona responsable en el proveedor, así como de la evidencia que justifique dicho cumplimiento.

b) Gestión de negocio. A continuación, se ha de evaluar (en mayor o menor medida) la gestión diaria de la privacidad por parte del proveedor, es decir se examinarán las medidas de seguridad implementadas y el cumplimiento de los requisitos del RGPD, como por ejemplo los mecanismos para el ejercicio de derechos.

En el artículo 28 ("Encargado del tratamiento") del RGPD, se especifica que el tercero ha de *"tomar las medidas necesarias de conformidad con el artículo 32"* (el artículo del Reglamento referente a la obligación de implementar las medidas técnicas y organizativas durante el tratamiento), por lo que es necesario implementar en las evaluaciones a terceros (y dejar evidencia) como mínimo las revisiones referentes a:

- "pseudonimizacion y cifrado de datos personales": En que ocasiones se utiliza cifrado de datos y/o pseudonimizacion por parte del proveedor de los datos personales (por ejemplo, en los entornos de pruebas, o cuando se trata de categorías especiales de datos).

- "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento": Qué medidas técnicas tiene implementadas el proveedor (por ejemplo, controles de seguridad, copias de seguridad periódicas, elementos en alta disponibilidad, sistemas de anti-malware, etc.)

- y "la capacidad de restaurar la disponibilidad y el acceso a los datos personales

de forma rápida en caso de incidente físico o técnico": La existencia o no de Planes de continuidad de negocio o desastre o procedimientos/políticas de copias de seguridad.

Este tipo de revisiones se podrán realizar mediante formularios que se hacen llegar al proveedor para que constaten las medidas y ellos certifiquen que son ciertas, o dependiendo del tamaño de la empresa y/o el proveedor y la criticidad de este, incluso con solicitud de evidencias resultado de los controles implementados (como, por ejemplo, informe de copias de seguridad, etc.)

c) Respuesta a incidentes. Otro de los puntos más importantes a la hora de evaluar a los proveedores es la gestión de incidentes de privacidad (cómo actuarían en caso de pérdida de datos o robo de información, por ejemplo). Será necesario evaluar si el proveedor cuenta con procedimientos al respecto y si están implementados correctamente los canales que permitan al responsable cumplir con los requisitos del RGPD, tanto en forma como en tiempo, en caso de que el incidente se produzca en el lado del proveedor.

d) Seguridad IT. Tal y como señalábamos, los proveedores, deben ofrecer garantías suficientes para aplicar medidas técnicas de manera que el tratamiento sea conforme a lo que exige el reglamento.

Estas medidas deberán ser revisadas por el responsable y cuyo alcance podrá incluir, entre otros, algunos de los controles que a continuación y a modo de ejemplo se enumeran:

- La existencia de un control de acceso a los entornos tanto a nivel físico como lógico mediante identificador único de usuario,
- Limitación los accesos por roles de funciones,
- Registro de accesos mediante logs (trazables),
- Conservación de datos pseudonimizados,
- Backups cifrados en entornos separados, y comunicaciones, utilizando redes VPNs basadas en IPSEC o SSL.

Las medidas también podrán ser validadas mediante garantías tales como certificados ISO/IEC como la norma 27001, para acreditar la seguridad en los sistemas de información, y más específicamente con la norma 27701 que contiene requerimientos adicionales de privacidad.

e) Gestión del personal. Se deberá comprobar que el personal del tercero que participe en el tratamiento de los datos además de las obligaciones identificadas por el responsable cumpla con las obligaciones establecidas por el proveedor que estarán reflejadas en la política de seguridad y procedimientos específicos del mismo.

Algunas de estas obligaciones podrían ser los planes que deben seguir sus empleados ante incidentes de seguridad, mantener el compromiso de actuar con confidencialidad y no divulgación de información sensible de terceros, además de incorporar buenas prácticas como: ser cuidadoso con las credenciales de acceso, uso adecuado del correo electrónico y dispositivos externos o destrucción de documentación de forma segura.

f) Subcontratación. Una exigencia del RGPD es la autorización previa y por escrito del responsable del tratamiento para que el proveedor pueda recurrir a otro encargado del tratamiento o subencargado. Previo a la fase contractual, se podrá establecer como criterio para la contratación con el responsable que los subencargados estén sujetos a las mismas condiciones que se apliquen al encargado entre ellas las medias de seguridad y obligaciones, anteriormente señaladas, las cuales se harán extensivas a toda la cadena de subcontrataciones que pudiera estar involucrada en el tratamiento.

En cualquier caso, las entidades que vayan a contratar con un proveedor que tras pasar el procedimiento de homologación no cumpla con los requisitos establecidos en el mismo, podrán proponer un plan de mitigación con el objetivo corregir las deficiencias y alcanzar los requisitos, o en última instancia descartar la contratación de este en los casos dónde el proveedor no ofrezca las garantías suficientes y resulte de manera manifiesta un riesgo para el responsable del tratamiento, lo que a su vez conllevaría en si mismo un incumplimiento de la norma europea y especialmente de la obligación de diligencia debida por parte del responsable. Dicho procedimiento, debe tener peso o entidad suficiente dentro de la organización de manera que, en ningún caso, las necesidades o conveniencias del negocio puedan obviar o restarle importancia a esta obligación de diligencia respecto a la protección de los datos de carácter personal.

05

Fase Contractual

5.1. Introducción. Cumplimiento del Art. 28 RGPD.

El Encargado del Tratamiento puede realizar todos los tratamientos que el Responsable del Tratamiento le haya encomendado formalmente y debe cumplir con las instrucciones de dicho Responsable, que es el único que puede variar las finalidades y los usos de dichos datos personales, teniendo que responder de ellos en todo momento.

Esa **dirección y control** que el Responsable ejerce sobre el Encargado deben de quedar bien delimitadas, de ahí que el RGPD haya optado por exigir a ambos que regulen su relación a través de un contrato de encargo de tratamiento (en adelante "CET") o de un acto jurídico similar que los vincule y, expresamente y como novedad destacada, exige su formalización por escrito, inclusive en formato electrónico.

Con la exigencia de la formalización por escrito del contrato de encargo de tratamiento establecida en el artículo 28, el RGPD se está asegurando:

(i) Que toda prestación de servicios con terceras partes sea analizada y se identifique cuáles de ellas suponen o implican un tratamiento de datos personales;

(ii) Que una vez identificado su existencia, se analice su naturaleza y nos hagamos las preguntas correctas sobre la relación jurídica existente entre las partes y cuál puede ser el nivel de riesgo del tratamiento de datos personales objeto del contrato, para cubrir sus debidas necesidades de protección;

(iii) Que en aplicación del principio de accountability que rige toda la normativa de protección de datos del RGPD, qué mejor evidencia de cumplimiento de su Art. 28 que su formalización en contrato o acto jurídico por escrito; y

(iv) Que la complejidad de las relaciones entre responsables y proveedores no suponga un obstáculo insalvable para determinar las responsabilidades y obligaciones de cada uno de los intervinientes en cada tratamiento de datos personales, abarcando todos los roles posibles: responsable, encargado y subencargado.

El artículo 28 RGPD establece que el CET debe contener como mínimo:

1. Una descripción suficientemente detallada del mandato al encargado del tratamiento: el objeto, la duración, la naturaleza y finalidad del tratamiento;

2. Una relación de medidas técnicas y organizativas adoptadas por el encargado del tratamiento;

3. Una descripción suficientemente detallada de los datos personales objeto del tratamiento: la tipología de datos y categorías de interesados; y

4. Las obligaciones y derechos de las partes.

En la práctica se pueden plantear distintas posibilidades de formalización de los CET: (i) independientes del contrato de prestación de servicios/obra/etc. que se suscriba con el Proveedor; (ii) formando anexo inseparable de los referidos contratos; y (iii) como acuerdos marcos de tratamiento de datos personales que se firmen entre Responsables y Encargados que mantienen relaciones habituales y, dentro de este grupo, especial mención a los convenios marcos intragrupo, suscritos entre todas las sociedades de un mismo Grupo de Empresas que habilitan los distintos tratamientos de datos personales entre ellas, incluidas las transferencias internacionales cuando se traten de compañías multinacionales .

Por último, también resulta importante evitar el riesgo de utilización de modelos y exigencias que solo quedarán en el papel del contrato, por no realistas o irrealizables. Cláusulas exigentes que no se exigen, contaminan la credibilidad del contrato y la verdadera intención de las partes, que ya no será la de su obligado cumplimiento.

5.2. Contenido mínimo de un CET

Como hemos mencionado, el artículo 28 del RGPD nos indica el contenido mínimo que debe cumplir todo CET, pero igualmente esta materia se encuentra regulada en el artículo 33 de la LOPDGDD y ha sido desarrollada por la AEPD en sus Directrices para la elaboración de contratos entre responsables y encargados del tratamiento[1].

A efectos prácticos, resulta fundamental la fase de negociación previa al contrato que se lleve a cabo entre las partes y establecer una operativa con las áreas negociadoras responsabilizándolas para que el contenido de los CET se cumplimente correctamente para cada servicio contratado con el proveedor, reduciendo al máximo las ambigüedades que pudieran producirse en la determinación de las responsabilidades y obligaciones del Responsable y Encargado. Además, en aquellos casos que resulte adecuado por las relaciones habituales existentes entre las partes, convendría suscribir un contrato marco de encargo de tratamiento de datos personales, que deje ya regulado de forma

[1]Agencia Española de Protección de Datos / Directrices para la elaboración de contratos entre responsables y encargados de tratamiento / Mayo 2018 (https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf)

estable las condiciones generales de los tratamientos de datos que se produzcan entre dichas partes para cada servicio contratado en el futuro, obligando tan solo a concretarlos en ofertas, pedidos posteriores, etc. De todos estos aspectos ya se ha tratado en el capítulo anterior, toda vez que se deben tener en cuenta en la homologación de los proveedores en la fase pre contractual. En este capítulo nos centramos en su formalización en el contrato.

A la hora de desarrollar este contenido mínimo puede resultar útil considerar los siguientes aspectos:

1. El CET debe identificar claramente (i) el contrato mercantil del que surge o forma parte como anexo, (ii) la normativa aplicable, así como (iii) las tipologías de datos, categorías de interesados, naturaleza y finalidades de tratamiento, e incluirse en un anexo específico.

2. La entidad encargada del tratamiento debe asumir contractualmente la responsabilidad en la formación en materia de privacidad de sus empleados; por ello, en aquellos supuestos en los que no esté garantizada esta formación o en aquellos casos en los que sea especialmente sensible el acceso a los datos personales por parte de estos trabajadores, deberá incluirse en el propio CET la exigencia de que el Encargado acredite directamente al Responsable que sus trabajadores, o al menos los directamente implicados en el tratamiento del que es objeto el CET, han sido debidamente formados en materia de protección de datos y han firmado una expresa cláusula de confidencialidad al efecto, y deje evidencia de la misma.

3. El Encargado del Tratamiento debe poner a disposición del Responsable su asistencia en la gestión de los derechos de los interesados, por lo que será necesario su reenvío en un plazo máximo de días determinado en el contrato y a una dirección de contacto específica, que permita su gestión en el periodo de un mes legalmente establecido. En caso de que sea el Encargado del Tratamiento el que vaya a gestionar directamente ciertos ejercicios de derechos, será recomendable tratar de llegar a un nivel de detalle en la forma en la que debe llevarlo a cabo, de cara a que las instrucciones del Responsable incluyan las pautas más relevantes a seguir por el Encargado. Deberá también quedar expresamente estipulado en el CET la exigencia y forma para el Encargado de acreditar al responsable de la gestión que se haga de dichos ejercicios de derechos durante toda la vida del CET.

4. Para dar cumplimiento al art. 32 RGPD, que exige al responsable y el encargado del tratamiento la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, analizado previamente por las partes en la fase pre-contractual, el CET no solo debería establecer concretamente qué medidas exigirá al encargado, normalmente en anexo, sino la comprobación presente y control futuro de las mismas por parte del responsable. En ocasiones, en función de cómo sea la prestación del servicio o la entidad del propio proveedor, la determinación de dichas medidas en el CET podrá ser sustituida por la acreditación por el encargado de Certificaciones de Seguridad o su adhesión a Códigos de Conducta. Para que sean realmente efectivas, y pueda evaluarse por la autoridad de control la responsabilidad de cada interviniente ante una posible violación de la seguridad de los datos personales, es importante que esas medidas sean acordadas previamente por ambos, responsable y encargado, en la fase pre-contractual, que no sean fruto de una mera imposición de una cualquiera de las partes y que estén ajustadas a la realidad del servicio a prestar, para lo cual se debe contar con el apoyo de las áreas de negocio que conozcan el detalle del servicio, y el área de seguridad de la información que pueda asesorar en su idoneidad al caso concreto.

5. El CET debe regular también la finalización de la prestación del servicio, tanto en el caso de que el responsable del tratamiento opte por solicitar la destrucción de los datos, de la que se debería exigir su debida acreditación, como en los casos de portabilidad, con la formalización de un protocolo de devolución y remisión a otro encargado. Este aspecto del CET será desarrollado con más detalle en el siguiente capítulo dedicado a la fase post-contractual.

6. El CET deberá establecer la obligación para el Encargado del Tratamiento de acreditar la existencia de procedimientos o políticas que regulen las posibles brechas de seguridad, auditorías o inspecciones, y que en todo caso recogerán la obligación de ponerlas en conocimiento del responsable por escrito, y en el plazo contractualmente establecido.

   Para la correcta gestión de posibles brechas de seguridad, el CET deberá dejar regulado en qué consistirán los compromisos de colaboración y participación activa en la gestión de la brecha de seguridad y en los planes de acción de cada Responsable y Encargado de Tratamiento, asegurando el cumplimiento por parte del responsable de su obligación de notificar en el plazo máximo de 72 horas, por lo que el plazo contractual para el encargado deberá ser el más breve

posible (preferentemente 24 horas), posibilitando además una pronta involucración de las áreas de ciberseguridad que permita confirmar en qué medida han podido verse impactados los propios sistemas de información de cada una de las partes; pero que al mismo tiempo, permita al encargado un margen de investigación interna y consensuar con el responsable la notificación a las autoridades o interesados, siempre que en esta se nombre de manera directa o indirecta al encargado.

7. En relación con la regulación de la subcontratación, es importante establecer en el CET (i) una operativa de comunicación de los subcontratistas al responsable del tratamiento y, si fuera necesario, autorización o al menos información, para que el responsable pueda, tras analizarlo, rechazar al nuevo subcontratista (p.e. en caso de que haya sufrido una violación de seguridad de los datos personales en el último año, etc.) y (ii) regular las potenciales transferencias internacionales de subcontratistas y las garantías que cubren dichas transferencias.

8. Especial mención de la regulación de la cláusula de auditoría, que trataremos en detalle en un apartado siguiente, una de las relevantes durante la negociación del CET, que saldrá del resultado de la negociación entre los intereses del encargado del tratamiento, con una periodicidad máxima (normalmente anual) y que el coste lo asuma el responsable, especialmente para la realización de auditorías externas, mientras que el responsable tratará de garantizar la colaboración del encargado y la eliminación del coste. Es importante vincular esta cláusula con la posibilidad de controles internos en los que participe la otra parte.

9. La regulación de la responsabilidad es uno de los temas más controvertidos en una negociación, si bien con el nuevo enfoque del RGPD que regula las obligaciones específicas de los Responsables y los Encargados y la responsabilidad de ambos, una posibilidad es tratar de llevar al contenido de la cláusula lo recogido en el art. 82 del RGPD. En el caso de los Responsables, es relevante tratar de no establecer una limitación de cantidad o que quede definido qué se está limitando y qué no puede limitarse por ser una responsabilidad directa administrativa del proveedor. Para un Encargado, sería conveniente indicar los casos en los que por seguir instrucciones del Responsable la responsabilidad debe recaer en éste y no sobre el Encargado que materialmente haya incumplido.

Es conveniente exigir al encargado de tratamiento que disponga de un seguro, aval u otro tipo de garantía de un adecuado ejercicio profesional -y su conserva-

ción durante la vigencia del contrato- lo cual facilitará al responsable del tratamiento el ejercicio de un derecho de repetición en caso de ser condenado.

10. En el caso de que la prestación de servicio no necesite acceso a datos personales, pero el prestador del servicio pueda acceder indirectamente a los mismos, no sería necesaria la firma de un CET, sino únicamente de una Clausula de Prestación de Servicio sin Acceso a Datos, es decir, de una cláusula de confidencialidad que obligue al proveedor en caso de que accidentalmente tenga acceso a datos personales durante el desarrollo de los servicios prestados. Una opción que se da en muchas ocasiones con los contratos marco, especialmente cuando se trata de proveedores que potencialmente podrían llegar a acceder a datos por el tipo de prestación de servicio, es el incluir por defecto la redacción de un CET, de manera que aplique por defecto la cláusula de confidencialidad (no acceso a datos) pero que en caso de que se llegue a materializar ese acceso, se contemplen ya las instrucciones para ese encargado circunstancial.

11. El CET puede acompañarse de diversos anexos: entre los que podríamos citar i) cuadro identificativo del tratamiento, tipología de datos, finalidad del tratamiento y categoría de los interesados; ii) relación de las empresas subcontratadas por el encargado de tratamiento, conteniendo el nombre de la entidad, la actividad subcontratada, ubicación y garantías implementadas; y iii) enumeración de las medidas de seguridad exigidas conforme al análisis de riesgo o de impacto realizado, y que habitualmente diferencia entre las medidas de seguridad de nivel bajo y las de nivel alto que aplicarán en determinadas circunstancias, como con tratamientos de datos especialmente sensibles. En el Anexo YY se ofrecen ejemplos de (i) y (ii).

5. 3. Aspectos Internacionales.

Una cuestión muy relevante a la hora de negociar contratos entre Responsables y Encargados del Tratamiento en un mundo globalizado como el actual, es la consideración de los aspectos internacionales que puedan existir. Algunos de ellos son:

Ámbito de aplicación territorial del RGPD (artículo 3):

Teniendo en cuenta los ejemplos que facilita el Comité Europeo de Protección de Datos ("EDPB" por sus siglas en inglés) en su guía sobre el ámbito territorial del RGPD[2], es ne-

[2]Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - version adopted after public consultation: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

cesario tener en consideración las siguientes situaciones:

- **Responsable del tratamiento con establecimiento en la Unión Europea, al que le resulta de aplicación el RGPD, si va a contratar a un proveedor que vaya a tratar datos en su nombre y por su cuenta como Encargado del Tratamiento, y este encargado está ubicado fuera de la Unión Europea**, tiene que asegurarse de firmar un contrato con todos los requisitos del art. 28 (3) del RGPD. En la práctica, el Responsable tiene que asegurarse de que el Encargado cumpla con las obligaciones del RGPD y, por tanto, podría llegar a considerar imponer contractualmente las obligaciones contempladas en el art. 28 (3) del RGPD a la otra parte.

  Desde un punto de vista práctico, la mayor parte de los prestadores de servicios de fuera de la Unión Europea y con gran impacto en el tratamiento de datos (p.e. proveedores de servicios de computación en nube, analítica, herramientas de atención al cliente, gestión de recursos humanos, etc.) que dirigen sus servicios a clientes corporativos (empresa) de la Unión Europea, ya contemplan en sus modelos de contratos o condiciones generales de contratación un clausulado específico orientado a cumplir con el art. 28 del RGPD.

- **Responsable de fuera de la Unión Europea, a cuyo tratamiento de datos personales no le resulta de aplicación el RGPD y que contrata a un Encargado del Tratamiento de la Unión Europea.**

  Será el Encargado del Tratamiento el que en este caso debe poner los esfuerzos en la negociación para cumplir con sus obligaciones como encargado del tratamiento conforme al art. 28.2, 3, 4, 5 y 6 del RGPD, es decir, todas salvo las de dar soporte al Responsable para que pueda cumplir con sus propias obligaciones bajo el RGPD.
  Esto podrá ser especialmente relevante en casos de prestadores de servicios europeos que dirijan sus servicios a entidades de fuera de la Unión, como grupos empresariales en los que la entidad que presta servicios como Encargado del Tratamiento del resto de entidades de fuera de Europa (por ejemplo, de gestión de recursos humanos en procesos de selección, o de soporte de atención al cliente), en este caso será la que centre sus esfuerzos en la negociación para incluir el clausulado conforme al RGPD.
  -En la práctica, desde la aplicación del RGPD, los modelos de contratos planteados desde el cumplimiento del art. 28 (3) del RGPD, se han venido considerando

internacionalmente como un modelo de contrato garantista y por tanto que se puede tomar como base en la negociación.

Regulación de las transferencias internacionales:

Son muchos los casos en los que pueden llegar a darse transferencias internacionales con motivo de la prestación del servicio de un Encargado y que habrán de haber sido objeto detallado de negociación entre las partes en la fase pre-contractual, dada su especial trascendencia. Algunas cuestiones relevantes:

- **Regular en el contrato la ubicación de las personas que van a prestar los servicios**, especialmetnte cuando estos puedan ser prestados en remoto, a través de teletrabajo o similar que permitan la ubicación del personal en un lugar distinto del de el establecimiento principal del proveedor.

  Este factor, que ha tenido un gran impacto durante la crisis sanitaria del COVID-19, es muy relevante a la hora de cubrir una potencial transferencia internacional motivada porque el encargado del tratamiento tenga empleados o subencargados localizados en territorios fuera de la Unión Europea para poder cubrir niveles de prestación de servicios (p.e. servicios relacionados con *call centers*, atención al cliente, soporte técnico, etc.).

- **La ubicación de los datos personales** es un factor clave a la hora de negociar el contrato (especial importancia en cuanto a la ubicación física de los servidores o *data centers* en contratos de computación en nube o tecnológicos), de cara a (i) recoger en el mismo que estarán ubicados en los territorios de la Unión Europea o considerados con protección equiparable y que esto sea una de las cuestiones a controlar durante la ejecución del contrato; o bien (ii) regular en el propio contrato la transferencia internacional, habitualmente mediante la inclusión de las cláusulas contractuales tipo en un anexo al contrato o documento independiente a firmar en un mismo acto con el CET, o si se tratase de una transferencia internacional por un tratamiento de un subencargado, que se incluya la autorización para firmar las cláusulas contractuales tipo o se incluya una referencia a las normas corporativas vinculantes si se tratase de entidades del mismo grupo empresarial.

  De cara a cubrir los riesgos por este tipo de casuísticas, es común solicitar a los Encargados del tratamiento una evidencia de las cláusulas contractuales tipo

que ha firmado con sus subcontratistas o una referencia a la publicación de la autoridad que ha aprobado las normas corporativas vinculantes.

Otros aspectos relevantes:

- De cara a facilitar la negociación del CET entre Responsable y Encargado del tratamiento con establecimientos en diferentes territorios dentro de la Unión Europea, puede resultar interesante tener en consideración los modelos de **cláusulas contractuales tipo** adoptadas por las diferentes autoridades europeas.

  La primera autoridad en adoptar y conseguir la publicación de su modelo por el EDPB ha sido la de Dinamarca[3], pudiendo considerarse su utilidad para partir de este documento en aquellas negociaciones que puedan resultar especialmente complejas o en las que los modelos de ambas partes puedan diferir mucho, para tratar de acercar posiciones de manera objetiva.

- La negociación con entidades que no son de la Unión Europea puede conllevar que los roles de Responsable y Encargado del Tratamiento se diluyan, ya que por ejemplo: (i) en Rusia ambas figuras son consideradas "data operator" y de ahí la importancia de establecer las obligaciones de cada parte en detalle en el contrato, para asegurarnos de que todos los puntos del art. 28 (3) se están recogiendo, con independencia de la denominación que se utilice en el contrato; (ii) la negociación con entidades de E.E.U.U en muchas ocasiones conlleva que el contrato recoja aspectos relevantes de privacidad en función del estado en el que esté ubicado el responsable o encargado, como el California Consumer Privacy Act ("CCPA")[4].

  En estos casos, es importante compatibilizar el clausulado del RGPD con el CCPA, porque si bien tienen aspectos comunes, son normas con enfoques muy diferentes y que necesitan cláusulas específicas para cada una. En la práctica, las referencias a cuando se traten datos personales a los que le aplique el RGPD se deberá cumplir con las cláusulas determinadas y cuando resulte de aplicación el CCPA aplicará la cláusula específica de la prohibición de la "venta" de datos (*do not sale)* y la regulación del Encargado del Tratamiento como un "prestador de servicios" tal y como se define en la normativa, conforme a las excepciones del CCPA para la transmisión de datos personales a terceros.

- El 16 de julio de 2020 la Gran Sala del Tribunal de Justicia de la Unión Euro-

[3] Artículo anunciando la publicación de las cláusulas y referencia a la opinión del EPDB y el documento: https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_en; https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-142019-draft-standard-contractual-clauses_en

[4] Referencia a las obligaciones para los "Service Providers" del apartado § 999.314. del CCPA: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf

pea (TJUE) publicó la esperada Sentencia del asunto C-311/18 Data Protection Commissioner v Maximilian Schrems, Facebooklreland (Schrems II). La Sentencia Schrems II decide sobre la conformidad con el Derecho de la Unión Europea y específicamente con el RGPD del Escudo de Privacidad UE-EEUU adoptado por la Comisión Europea en su Decisión 2016/1250 ("Escudo de Privacidad"), así como de las Cláusulas Contractuales Tipo para la transferencia internacional de datos recogidas en la Decisión 2010/87 ("Cláusulas Contractuales Tipo" o "CCT"). El TJUE declara inválido el Escudo de Privacidad, que establecía condiciones para garantizar un nivel adecuado de protección en las transferencias de datos personales a las empresas que traten los datos en los Estados Unidos y se hubieran adherido a este mecanismo. Por otra parte, el TJUE confirma la validez, con ciertas restricciones, de las CCT. Los Responsables y Encargados del Tratamiento deberán dar seguimiento tanto a las preguntas frecuentes publicadas como al grupo de trabajo que ha puesto en marcha el Comité Europeo de Protección de Datos para generar recomendaciones sobre cómo identificar e implantar medidas adicionales en caso de transferencias internacionales que utilicen las CCT.

5. 4. Controles periódicos. Seguimiento del cumplimiento de los términos de un CET.

Buscar mejoras en el proceso de desempeño específico de los encargados de tratamiento, ayudará al Responsable del Tratamiento a crear relaciones duraderas y desarrollar las competencias de ambas partes en un ambiente de confianza y cumplimiento. **Seguimiento y Control**, estos dos conceptos son una excelente combinación para poder disminuir o evitar problemas con nuestros proveedores, que deberán constar expresa y detalladamente en cada CET para hacerlos exigibles a las partes.

Entre las herramientas que disponemos para promover una política de relaciones con los proveedores basada en los principios de la ética empresarial y la transparencia, procurando la búsqueda de la mejora continua y el beneficio mutuo, destacan dos controles:

1. Auditorías.

El área o departamento asignado para realizar las funciones de auditoría, control y riesgos en materia de protección de datos y privacidad, será quien evalúa, de forma independiente, la razonabilidad y suficiencia del diseño y del funcionamiento de las opera-

ciones llevadas a cabo por los terceros. Esta función puede desarrollarla el Responsable por sí mismo o a través de terceros.

A petición del responsable del tratamiento, el encargado deberá poner a su disposición toda la información necesaria para acreditar que cumple con sus obligaciones contraídas mediante el CET y, más en general, las establecidas por la Legislación de Protección de Datos.

En caso de que la auditoría revelase un incumplimiento de una obligación por parte del encargado del tratamiento, el Proveedor deberá poner en marcha, planes de acción que le permitan mejorar los aspectos identificados como no conformes, para de este modo subsanar el defecto en un periodo acordado por las partes. Si se diera esta situación, el responsable podría cargar los costes de la auditoría durante la cual se detectaron las discrepancias en el encargado.

Si lo anterior no fuera posible, Responsable y Encargado podrán estar interesados en incluir en el propio CET referencias a certificaciones (p.e. PCI DSS para el caso de tratamientos que impliquen datos de tarjetas bancarias) o similares que sustituyan a la auditoría como revisión presencial, o exigir la realización de auditorías internas al encargado y que traslade el resultado de las mismas al responsable.

2. Evaluaciones continuas del desempeño que analicen el trabajo realizado y sirvan para completar la información del proveedor en el caso de que tenga que volver a ser calificado:

Las evaluaciones de desempeño establecen un proceso de valoración sistemática y documentada de los aspectos más significativos de la relación con los Encargados del Tratamiento.

A través de las evaluaciones de desempeño se identifican situaciones de riesgo potencial. Con ellas buscamos:

- Medir cuantitativamente el desempeño, para que la toma de decisiones tenga la mayor objetividad posible.
- Contar con una herramienta para mantener o modificar el estado de calificación del proveedor que hemos medido en el momento previo a la contratación.

- Considerar criterios adicionales a tener en cuenta en la futura selección de proveedores para la participación en peticiones de oferta.

Para una mayor eficiencia en la gestión de estos controles, debemos tener en consideración el formato en el que se van a solicitar, la herramienta, aplicación o similar a través de la que se van a gestionar las evidencias remitidas por los Encargados del Tratamiento, así como la colaboración y coordinación con las áreas de negocio que van a beneficiarse de la prestación de servicios, las áreas jurídicas que puedan requerir también un control de la subcontratación del proveedor, y cualquier otra área implicada en el desarrollo del servicio, en particular Seguridad de la Información y Tecnología de la Información por su control sobre las medidas de seguridad, para que los controles vayan integrados con sus propias auditorías y revisiones de la ejecución del contrato y la privacidad no sea un aspecto aislado en la revisión

.

Algunas medidas preventivas, que al incluirlas expresamente en el clausulado de los CET nos ayudan a mitigar los riesgos en nuestros Proveedores-Encargados y a garantizar el cumplimiento de los términos y condiciones establecidos en nuestros CET, son:

- Caso de **Subencargados de Tratamiento**, deberán poner a disposición del Encargado la información necesaria para demostrar el cumplimiento del contrato, **permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento**.

- Implementar un proceso de verificación, evaluación y valoración periódica de la eficacia de las medidas técnicas y organizativas que se hayan incluido en el CET, requiriéndose **el envío y actualización**, a lo largo del ciclo de vida del contrato, **de certificaciones en protección de datos y ciberseguridad, renovación de ISOS, resultados de auditorías, códigos de conducta, EIPDs / DPIAS, etc**.

- **Obligación para los Encargados de Tratamiento de organizar sesiones formativas periódicas entre sus empleados, para explicar todos los procedimientos y normativa interna**, lo que permite reforzar también una cultura de seguridad y privacidad.

- Establecer la realización periódica de una **encuesta de satisfacción del proveedor**, que proporcione la percepción que se tiene del mismo, con el fin establecer una mejora en su nivel de calidad o redunde como experiencia en beneficio de los procesos de selección de proveedores.

- **Establecer planes de desarrollo de proveedores** con el objetivo de conseguir que dicho proveedor alcance un mejor nivel de calidad requerido por el Responsable del tratamiento, fomentando la competencia con la entrada de nuevos proveedores.

- Establecer un control específico, en colaboración con las áreas de negocio que hayan estado a cargo del desempeño del proveedor y de las áreas jurídicas o de gestión documental que puedan controlar los plazos de terminación de los contratos, de cómo se lleva a cabo el protocolo de devolución, destrucción o entrega a un nuevo encargado de los datos personales objeto de la prestación de servicios. Este aspecto se tratará más detalladamente en el siguiente capítulo.

5.5. Toma de decisiones sobrevenidas ante situaciones imprevistas (tanto externas como internas).

Tanto en el momento de fijar las estipulaciones del CET como durante toda la vida del mismo, el Responsable y Encargado deberán tener en cuenta que sus actos podrán ser considerados un cumplimiento o incumplimiento de las normas que lo rigen: (i) normas administrativas que rigen el contenido y cumplimiento de estos CET, RGPD y LOPDGDD; y (ii) el principio de autonomía de la voluntad en los contratos del artículo 1.255 del Código Civil.

Las cláusulas que rijan las obligaciones entre Responsable y Encargado en los CET, siempre estarán condicionadas por la normativa sobre protección de datos personales y el régimen sancionador por su incumplimiento, en función de su gravedad, de conformidad con lo establecido en la LOPDGDD: **Infracciones graves**: (i) contratar a un encargado que no ofrezca garantías suficientes (art 73 j); (ii) encargar el tratamiento a un tercero sin haber formalizado antes un contrato o un acto jurídico por escrito (art. 73 k); (iii) que un encargado contrate a otros sin contar con la autorización o información previa del responsable (art. 73 l); (iv) la infracción al determinar los fines y medios del tratamiento (art. 73 m) cambiando la consideración del encargado a responsable (RGPD art. 28.10); e **infracciones leves**: (v) no informar al responsable sobre la posible infracción de la normativa sobre protección por una instrucción recibida de este (art. 74 j); y (vi) el incumplimiento de las estipulaciones del contrato u otro acto jurídico que regula el tratamiento o las instrucciones dadas por el responsable, salvo que esté obligado por la normativa y lo hubiera advertido al responsable o al encargado del tratamiento (art. 74 k).

En consecuencia, el CET deberá establecer directrices de cómo actuar entre el Respon-

sable y el Encargados antes las situaciones imprevistas: (i) consultas a las Autoridades de Control; (ii) apertura de expediente o sanción por parte de las Autoridades de Control; (iii) brechas de seguridad; (iv) modificaciones significativas en la prestación del servicio; (v) extinciones o fusiones, cambios de denominación social, cesiones, etc.; (vi) oposición a las auditorías u otros controles o resultados de esas auditorías/controles que resulten en la detección de un riesgo para el tratamiento de los datos personales objeto del contrato; y (vii) potencial arbitraje tecnológico.

06

Fase Poscontractual

La Fase Poscontractual es la última de las fases asociadas a la gestión de riesgos de terceros y está relacionada con la finalización de la prestación de servicios.

El cómo se lleve a cabo esta fase y lo que se pueda hacer al respecto, estará directamente condicionado por lo que se haya establecido previamente, bien en la RFP asociada a la licitación del servicio o bien en el propio contrato que se hubiera negociado entre las partes en el momento de adjudicación. Por eso, tal y como se ha mencionado en el apartado relacionado con la fase contractual, es sumamente importante que, en ambos casos, se hayan incluido aspectos concretos relacionados con la Finalización del Contrato, aspectos que tendrán mayor relevancia en función del nivel de riesgo de proveedor o incluso del impacto que pueda tener el servicio en la continuidad del negocio de la entidad.

De igual modo, es en dicho contrato donde se habrá tenido que establecer el momento en el comenzaría esa fase poscontractual ya que, sobre todo en aquellos servicios o contrato que supongan un traspaso con otro proveedor, es necesario contemplar previamente dicho traspaso y sería en ese momento cuando se podría considerar que comienza la fase poscontractual. De igual modo, como se menciona en el apartado asociado a la fase contractual, cobra especial relevancia los mecanismos que se hayan establecido para la devolución o destrucción de la información en esta fase de finalización del servicio.

En cualquier caso, en esta fase poscontractual, habrá que tener en consideración una serie de requisitos específicos que dependerán en su mayor medida en función de cómo haya sido la finalización del servicio y la importancia o relevancia del servicio y/o proveedor afectado.

De este modo, la finalización del contrato se podríamos clasificar en dos grandes bloques:

- Terminación del contrato planificada:
  - Finalización del periodo contractual acordado.
  - Por cese de la necesidad de la contratación del servicio.

- Terminación del contrato no planificada:
  - Por incumplimiento del contrato o de las disposiciones legales o regulatorias.
  - Por la ocurrencia de algún incidente.
  - Por cese del servicio por parte del proveedor.

- Por existencia de conflicto de intereses

6.1. Controles y garantías mínimas asociadas a la finalización del contrato

En la finalización de todo contrato con un proveedor que trate datos de carácter personal, habrá que tener en consideración una serie de controles y garantías mínimas:

- **Supresión o devolución a la entidad de todos los datos personales que haya estado tratando para él**: en virtud del apartado g) del párrafo 3 del artículo 28 del RGPD ("Encargado del Tratamiento"), el contrato debe estipular que a la finalización de la prestación el encargado del tratamiento deberá suprimir o devolver al responsable del tratamiento todos los datos personales que haya estado tratando para él. Es el responsable, según el mismo artículo, el que decide si se suprimen o se devuelven estos datos, estando estipulada por tanto en el contrato la decisión al respecto.

  Además, también estipula el citado artículo que deberá **suprimir todas las copias existentes de los datos personales**, a menos que la legislación de la UE o de los Estados miembros exija que se almacenen.

  Es importante señalar que la **supresión de los datos personales debe hacerse de manera segura**, de conformidad con los requisitos de seguridad del artículo 32 pudiendo solicitarse el correspondiente Certificado de Destrucción, si así se considera necesario El contrato debe incluir estos términos para asegurar la protección continua de los datos personales después de que el contrato termine. Esto refleja el hecho de que, en última instancia, es el responsable del tratamiento quien decide qué debe suceder con los datos personales que se están procesando, una vez finalizado el tratamiento. En el caso de que no sea posible que los datos de las copias de seguridad o de los archivos se eliminen inmediatamente después de la terminación de un contrato es necesario que se establezcan las **salvaguardas adecuadas** y se garantice que son convenientemente eliminados tan pronto como sea posible.

- Transferencia del conocimiento: es importante que a la finalización del servicio el proveedor transfiera el conocimiento adquirido o generado durante la prestación del servicio a la organización o hacia el proveedor que ésta designe, sin que ello repercuta en una pérdida del control o del nivel de calidad del servicio.

- En el caso de los contratos de Cloud Computing, es especialmente relevante la regulación de la portabilidad de los datos a la finalización del contrato, conforme a lo indicado por la AEPD en su guía[5], y en función del tipo de servicio a regular (p.e. aquellos que impliquen la completa migración de una base de datos de clientes o usuarios para el envío de comunicaciones comerciales), puede ser relevante la formalización de un protocolo de devolución y remisión a otro encargado.

- Traspaso de documentación: el proveedor deberá traspasar a la entidad o al proveedor entrante toda la documentación y datos que se haya generado durante el periodo de prestación de servicio.

- Garantía del deber de confidencialidad: es necesario garantizar que el deber de confidencialidad del proveedor se mantiene incluso una vez finalizada la relación contractual ya que así se evita, entre otras cosas, que la información obtenida durante la prestación pueda ser difundida o utilizada.

- Eliminación de los permisos de acceso del proveedor: Otro aspecto a tener en cuenta es la gestión de accesos tanto físicos como telemáticos. En caso de que el servicio subcontratado se haya llevado a cabo en la sede del cliente, se retirará el acceso a esta y si el acceso por parte del proveedor se ha realizado a los sistemas de la empresa, este también deberá ser anulado, evitando así que puedan acceder a cualquier recurso interno una vez el contrato ha finalizado.

  Adicionalmente, en el caso de que la finalización del servicio sea no planificada, se deberá tener en consideración una serie de controles adicionales:

- Implantación de controles temporales: se deberán implementar controles temporales durante la finalización del servicio que permitan minimizar el impacto que este tipo de terminaciones pueda llevar asociadas. Como por ejemplo cómo actuar en el ejercicio de derechos por parte de usuarios que tienen relación directa con el proveedor, accesos lógicos o físicos necesarios durante el periodo de transición, etc.

- Análisis sobre la privacidad: sería conveniente realizar un análisis interno sobre la privacidad para garantizar que los derechos con respecto a la protección de datos de los usuarios afectados por el tratamiento del proveedor "saliente" se siguen manteniendo tanto si el proveedor es sustituido, como si lo es o durante

[5] https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf

el periodo de transición (por ejemplo donde han de ejercer sus derechos, si las medidas temporales de seguridad como donde se almacenan los datos "devueltos" son adecuadas, etc.).

6.2. Controles y garantías adicionales en el caso de finalización del contrato por incumplimiento

En el caso de que se vaya a producir una finalización del servicio no planificada y asociada a un incumplimiento, es importante que aparte de los controles y garantías mínimos detallados anteriormente se tengan en consideración una serie de aspectos adicionales:

- **Revisión de las cláusulas del contrato:** antes de comenzar con todos los trámites es necesario revisar el contrato a fin de confirmar si contenía disposición relativas a la terminación y si se regulaba de algún modo la forma o los motivos por los que se puede terminar el contrato.

- **Identificación de los incumplimientos asociados:** deberá identificarse y documentarse específicamente y de manera clara los incumplimientos que se han producido por parte del proveedor y que derivan en la finalización del contrato.

- **Aviso de rescisión del contrato:** será necesario el aviso por escrito para cualquier tipo de terminación y mucho más en este caso. Este aviso deberá realizarse de acuerdo a cómo se haya establecido en el contrato (por ejemplo, por correo certificado, correo postal, correo electrónico, burofax, ...) y teniendo en cuenta el periodo de preaviso que se haya establecido. La notificación debe incluir la razón de poner fin al contrato y una referencia al párrafo del contrato en que se habla de la resolución.

- **Control sobre el traspaso del servicio y transferencia del conocimiento:** en este tipo de terminaciones, dado que las relaciones suelen estar afectas, se hace mucho más importante mantener un control sobre el adecuado traspaso del servicio y transferencia del conocimiento para garantizar que no se pierde información en el proceso.

En estos casos, es muy relevante la colaboración con las áreas de negocio que han contratado la prestación de servicios, de cara a poder determinar en qué casos será más conveniente ejecutar el contenido de las cláusulas de resolución del contrato y resolver anticipadamente el mismo, o en cuales se deberá articular una solución de otra índole,

mediante lo indicado en los controles internos para la subsanación del incumplimiento por parte del encargado y la monitorización de la evolución por parte del responsable. Es importante que quede todo perfectamente documentado a fin de poder acreditar en todo momento tanto la debida diligencia del Responsable del Tratamiento como las decisiones y actuaciones llevadas a cabo.

6. 3. Controles y garantías adicionales asociados a la finalización del contrato de proveedores estratégicos o de riesgo alto.

Especialmente en el caso de proveedores estratégicos o considerados de riego alto, será importante implementar controles y garantías adicionales para garantizar el impacto a la privacidad y protección de datos que esta finalización lleva asociada, así como establecer mecanismos de trazabilidad para dejar constancia del cumplimiento.

A continuación, se detalla una lista de controles adicionales mínimos a tener en cuenta (lista no exhaustiva):

- **Garantía de la devolución de los datos o supresión de los mismos:** mediante una declaración por parte del Encargado o de un tercero, una auditoria interna, una declaración de borrado seguro o cualquier otro control pactado. Se debe comprobar por parte del Responsable (y dejar trazabilidad para poder demostrar) que el borrado se ha realizado de manera segura.

- **Garantía del borrado de las copias de seguridad** o controles establecidos para borrado en un tiempo estipulado.

- **Análisis de todos los accesos asociados al proveedor:** en caso de que el proveedor tuviera acceso a sistemas o datos del Responsable para la realización del tratamiento, realización de un análisis de todos los accesos (VPN, enlaces de comunicaciones, accesos físicos por parte del personal, etc.), usuarios y permisos creados para tal fin a fin de identificar todas las acciones que puedan ser necesario para garantizar la eliminación de todos esos permisos.

- **Control del material cedido al proveedor:** identificación del material de la empresa cedido al proveedor para la prestación del servicio y control sobre la devolución de los mismos.

- **Control de los accesos de la empresa a los entornos y sistemas del proveedor:** en el caso de que la empresa igualmente tuviera acceso al entorno del proveedor, será necesario también analizar usuarios, material, accesos y permisos y garantizar la eliminación y/o devolución de los mismos.

6. 4. Responsabilidad legal asociada al proveedor en caso de incumplimiento

Por el impacto que puede tener un incumplimiento por parte del proveedor de la normativa de protección de datos, se hace necesario tratar expresamente esta situación identificando las posibles acciones que puedan llevarse a cabo.

Lo primero que ha de tenerse en cuenta es que el propio considerando 146 del RGPD establece que *"el responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento"* y posteriormente, ya en el artículo 82, se concreta este derecho del afectado a ser indemnizado y la responsabilidad de responsables y encargados del tratamiento.

Por otra parte, es necesario recordar que este derecho a percibir una indemnización no es exclusivo del RGPD ni novedoso; actualmente existen otras vías legales en vigor para que los afectados puedan reclamar indemnización por los daños y perjuicios causados a los afectos, como la responsabilidad contractual o extracontractual prevista en el Código Civil o la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Respecto a los daños y perjuicios que puede sufrir una persona y que generan su derecho a ser indemnizado deben entenderse en un sentido amplio, según indica el propio RGPD que justifica en su exposición de motivos esta previsión en la jurisprudencia del Tribunal de Justicia de la Unión Europea. Esto significa que no son sólo los daños materiales, también los inmateriales o morales. Los primeros, los materiales, son más fácilmente cuantificables, pero en el ámbito de la protección de datos nos solemos mover más en el segundo entorno, en el de los daños morales, cuya cuantificación es más complicada. De hecho, no hay unos baremos que puedan servir de referencia, aunque sí se puede afirmar que los datos más sensibles serán los que generen indemnizaciones más elevadas (por ejemplo, difusión ilícita de datos ideológicos, sexuales, salud, religiosos, inclusión indebida en registros de solvencia… sin olvidar el derecho al honor y la intimidad, o el más novedoso derecho al olvido digital).

El reparto de Culpas

Ya no es sólo el responsable del tratamiento el culpable frente al afectado, conforme a RGPD todos los intervinientes en el tratamiento; responsables, corresponsables y encargados, responden frente a aquel de los daños y perjuicios causados que hayan participado en la misma operación de tratamiento.

Es más, para garantizar que el afectado pueda recibir una indemnización efectiva, cada uno de dichos intervinientes será responsable de todos los daños y perjuicios causados, sin perjuicio del derecho de repetición del que haya tenido que pagar la indemnización frente a los demás, pudiendo reclamar la parte proporcional frente a cada uno de ellos. Aquí la solvencia va a ser determinante: el afectado, en el supuesto de que obtenga una resolución judicial que reconozca su derecho a ser indemnizado, se dirigirá al deudor más solvente, que no necesariamente es el responsable, puede ser perfectamente el encargado del tratamiento, recordemos que actualmente hay prestadores de servicios (por ejemplo, tecnológicos o en la nube) que superan exponencialmente su valor y su volumen de negocio al de los propios responsables. Por tanto, habrá que prestar especial atención a las cláusulas de limitación o exención de responsabilidad y a las garantías o solvencia que puedan ofrecer las partes intervinientes en el tratamiento de datos personales.

La exención de responsabilidad

Tanto responsable como encargado del tratamiento podrán eludir esta responsabilidad si son capaces de acreditar que en modo alguno son responsables de los daños causados. Aquí volvemos al principio de responsabilidad proactiva y a la privacidad desde el diseño y por defecto, que exigirá que el responsable y el encargado cumplan y sean capaces de acreditar su cumplimiento, debiendo conservarse evidencias de todas las actuaciones realizadas al respecto, puesto que, en caso de no ser capaz de acreditar esta diligencia, será responsable por los daños y perjuicios causados.

.

07

“Otras terceras” partes

7.1. Escenarios de relaciones con "otros terceros"

En este apartado, "otros terceros", analizaremos, desde una perspectiva práctica, y que podemos ver todos en nuestro día a día, aquellas relaciones con terceros, algunas complejas de identificar dentro del contexto de la normativa de protección de datos, al ser distintas de las habituales responsable encargado analizadas en los capítulos anteriores.

- **Relaciones entre corresponsables del tratamiento (*"joint controllers"*)**: cuando hablamos de corresponsables del tratamiento (art 26 RGPD y art 29 LOPD y GDD), nos estamos refiriendo a dos organizaciones independientes pero que determinan conjuntamente (*joint)* los objetivos, fines y medios aplicables al tratamiento de datos. Este tipo de situaciones se produce porque ambas empresas deciden los medios y la finalidad del tratamiento y, ambas, acuerdan las responsabilidades que les pudieran corresponder en relación con dicho tratamiento de datos personales. Como ejemplo de este supuesto, la LOPDGDD dispone en su artículo 20, apartado 2, dentro del tratamiento de datos del "Sistema de Información crediticia" que las entidades que mantengan el sistema de información crediticia con datos relativos al incumplimiento de obligaciones (dinerarias, financieras o de crédito) y las entidades acreedoras, respecto al tratamiento de los datos relativos a sus deudores, tendrán la consideración de corresponsables (*joint controllers*) del tratamiento de los datos, siendo de aplicación para ambas entidades lo dispuesto en el artículo 26 del RGPD.

- **Relaciones entre responsables separados e independientes (*"controller to controller"*):** serán responsables separados e independientes, aquellas relaciones que se dan entre dos organizaciones independientes que pueden intercambiar datos personales, pero ninguna de las partes participa en la determinación de los medios o finalidades de la otra parte. En otras palabras, no determinan conjuntamente los objetivos, fines y medios y ni las responsabilidades que les serían aplicables. Como ejemplo de esta situación, podría citarse la relación existente y las distintas responsabilidades (como *"controllers"* o responsables independientes) que se producen entre una compañía aseguradora y la correduría de seguros, cuya determinación viene recogida en la normativa que regula dicha actividad[6]. Así, entre otras, cuando el corredor obtiene los datos personales de su cliente (posible tomador del seguro) y los comunica a la aseguradora para formalizar la póliza con el tomador, ambas partes deben cumplir de manera separada e independiente (como "Responsables"), con las obligaciones que, en materia de protección de datos, les resulten aplicables.

[6] Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.

- **Relaciones con terceros "ambivalentes" (*"controller" and "processor"*):** esta situación, se produce cuando dentro de las diferentes fases de un servicio, el tercero actúa en un tramo o fase como responsable y en otro tramo como encargado. Como ejemplo de esta situación, podemos señalar algunas relaciones que podrían tener lugar en el sector publicitario entre el anunciante, la agencia de medios y el medio (soporte). En determinadas situaciones una agencia podría ostentar el rol de "Encargado" al que el anunciante le ha encomendado recabar datos de usuarios a partir de diferentes medios (páginas web, redes sociales, etc.); y a su vez podría ser "Responsable" cuando utiliza dichos datos para sus propios fines (p.e. enriquecer sus propios perfiles de audiencia o segmentos) a partir de la información obtenida mediante la aplicación de sus propias tecnologías de medición y seguimiento de campaña.

- **Relaciones con terceros "intermediarios" que no acceden a datos personales:** en estas relaciones estamos ante terceros que actúan como meros intermediarios que, aunque no intervienen directamente en el tratamiento de datos personales, actúan bajo el mandato /servicio de procurar en nombre y por cuenta de su mandante (contratante), los servicios de otras entidades que, si tratarán los datos personales, en condición de encargado o responsable. Imaginemos, como ejemplo, un contratista al que se le encomienda, únicamente, "acercar a las partes", proponiendo a su mandante opciones para la contratación con terceros intermediados por éste. El intermediario actúa bajo comisión y realiza un servicio como intermediario entre su mandante y el tercero cuya contratación haya procurado, pero no interviene directamente en el tratamiento de datos que se desprenda de dicha intermediación.

7. 2. Recomendaciones en la fase previa a la contratación con "otros terceros".

Antes de constituir una relación contractual con los terceros cuyas características fueron descritas en el apartado anterior, conviene realizar un ejercicio de debida diligencia para tener mayor claridad sobre el tratamiento de datos que será efectuado por cada parte, así como sobre la naturaleza de su intervención. A tales efectos, a continuación, se apuntan algunas recomendaciones y buenas prácticas:

- **Determinar la naturaleza y el alcance los servicios:** previo a la contratación, es necesario asegurarse de que la oferta o propuesta de servicios detalle, clara y suficientemente, el alcance y las características de las prestaciones del tercero,

evitando cualquier ambigüedad o generalización con respecto a las actividades que serán efectuadas. La determinación concreta de tales prestaciones nos permitirá advertir, anticipadamente, si los servicios propuestos están "encauzados" dentro de las expectativas asociadas a la propia naturaleza y/o servicio del tercero o si, por el contrario, existen prestaciones "no naturales" que conviene identificar, añadir y regular dentro del flujo de tratamiento de datos.

En algunos sectores este tipo de cautelas requiere especial atención. Por ejemplo, en el sector asegurador, la naturaleza de los servicios y el rol de "Responsable" atribuible a una correduría, viene determinado por la normativa que regula su actividad intermediadora[7]. Durante la configuración de los servicios entre aseguradora y correduría (ambos "Responsables" independientes (*"Controller to Controller"*), si, por ejemplo, existiera alguna prestación de servicios adicional que pueda exceder a las habituales de la correduría o fueran realizadas al margen de su actividad regulada (p.e. gestión de siniestros derivados de la póliza), esta prestación adicional debería analizarse separadamente para determinar su viabilidad (según normativa sectorial) así como su implicación en la normativa de protección de datos personales, ya que podrían modificar la "expectativa habitual" sobre su rol/condición como "Responsable del Tratamiento".

- **Determinar mapa/flujo del tratamiento de datos:** una vez determinado el alcance y naturaleza de los servicios propuestos, es necesario realizar un ejercicio de "cartografía" del tratamiento de datos derivado del servicio, estableciendo un mapa exhaustivo de las actividades que serán realizadas que incluya, entre otros, los tipos de datos utilizados y los flujos de información e intervenciones de cada parte[8]. Por ejemplo, en el sector sanitario puede darse cierto flujo de datos (proporcional y limitado a determinar el importe de la prestación sanitaria realizada) entre un centro sanitario y una entidad aseguradora (ambos "Responsables" separados e independientes). La falta de claridad sobre el alcance de dicha comunicación, quién será el propietario del canal/medio de transmisión, quién deberá aplicar las medidas de seguridad que correspondan en cada fase y bajo qué criterios/protocolos, etc., podría obstaculizar la determinación contractual de las obligaciones y responsabilidades atribuibles a cada una de las partes, en los tramos del tratamiento que les correspondan.

- **Determinar naturaleza y condición de las partes implicadas:** partiendo del mapa de tratamiento de datos que hemos identificado, así como el alcance y naturaleza de sus servicios, es necesario establecer el rol o condición atribuible

[7] Art. 203 del Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.

[8] Si la propuesta de servicios resulta insuficiente para determinar los flujos de tratamientos de datos que tendrán lugar en cada fase del servicio, podrían utilizarse cuestionarios complementarios para recabar dicha información y completar el análisis.

al tercero, ya sea durante el servicio o en cada una de las fases/tramos de su prestación. Este ejercicio es fundamental para evitar: (i) asignar una condición errónea al tercero, designándolo, por ejemplo, como "Encargado" cuando por normativa sectorial o por la naturaleza de su servicio debería ostentar el rol de "Responsable"; y (ii) regularizar erróneamente situaciones en las que un mismo tercero podría ostentar una condición "ambivalente", es decir, ostentando el rol de "Encargado" en determinadas fases/tramos del servicio y a su vez el rol de "Responsable", con respecto a otras prestaciones o tramos del tratamiento de datos incluidos en el mismo servicio.

A modo de ejemplo: en el sector publicitario, existen servicios realizados en entornos digitales, en los que pueden intervenir múltiples actores (p.e. anunciantes, agencias, *publishers*, editores de contenidos, proveedores de tecnologías publicitarias de seguimiento/ medición, etc.) quienes en los diferentes "tramos" del servicio podrían ostentar la condición de "Responsables" o de "Encargados" en función de su capacidad para determinar los medios/finalidades aplicados al tratamiento de datos obtenidos a partir de cookies, píxeles o tecnologías similares.

Tales situaciones han sido advertidas por la propia AEPD al señalar[9]: *"Así, anunciantes, editores, agencias, redes publicitarias y otros agentes intervinientes serán responsables del tratamiento cuando utilicen cookies propias y cuando, utilizando cookies de terceros, participen en la determinación de los fines y medios del tratamiento, aunque este se realice a través de un encargado del tratamiento, como por ejemplo cuando un anunciante contrata a una agencia de medios para que realice los tratamientos bajo su dirección y de acuerdo con sus instrucciones (…) En principio, cada responsable del tratamiento responderá del tratamiento concreto que realice. Incluso en aquellos casos en los que concurran diferentes responsables del tratamiento, cada uno de ellos asumirá su respectiva responsabilidad"*.

- **Solicitar garantías de cumplimiento previas a la contratación:** en este apartado cabe advertir que previo a solicitar cualquier tipo de garantías habría que analizar "caso a caso" el carácter de la relación establecida con el tercero. Es preciso recordar que los "otros terceros" a los que nos referimos no son típicos "Encargados" de los que se pueda "requerir" ciertas "garantías estandarizadas" por imperativo legal, sino que se trataría de *"partners"* cuya posición contractual podría ser más "equitativa" o de entidades que tratan datos bajo sus propias finalidades y disponiendo de sus propios medios. Por tanto, nuestro análisis no

[9] Guía para el uso de las Cookies (p.32). https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

podría derivar en un "requerimiento estándar" (tipo *checklist)* aplicable a todas las contrataciones sino en un verdadero ejercicio de "debida diligencia", considerando, en cada caso, los elementos particulares de la naturaleza/alcance del servicio, mapa/flujo de datos y prestaciones, condición/rol del tercero en cada fase/tramo del tratamiento previsto.

A modo de ejemplo, habría situaciones en las que se contrate el servicio de un tercero para incluir anuncios publicitarios en sus entornos digitales (p.e. red social, página web, app, etc.) con el fin de impactar audiencias/segmentos predeterminados en función de características/perfiles de sus usuarios. En tales casos, podría solicitarse que dicho tercero acredite que dispone de mecanismos idóneos para recabar el consentimiento inequívoco de dichos usuarios (para creación de perfiles, uso de cookies propias y/o de terceros, con fines publicitarios y/o de medición de campañas, etc.). A tales efectos, se podría considerarse la adhesión del tercero a códigos de conducta o estándares sectoriales[10].

Para otro tipo de prestaciones, quizás convendría solicitar al tercero certificaciones de cumplimiento de normas o estándares reconocidos y aplicables a su actividad o sector, que resulten relevantes para el tratamiento de datos previsto, por ejemplo: normas de la familia ISO 27001 o similares[11] (seguridad de la información, ciberseguridad, etc.); normas PCI-DSS[12] (pasarelas/medios de pago); códigos de conducta o códigos aplicables al tratamiento de datos en su actividad[13], etc. Finalmente, todo lo anterior no excluye que, en ciertos casos, puedan solicitarse las "garantías habituales" que permitirían acreditar que el tercero ostenta un grado óptimo de madurez o cumplimiento normativo, por ejemplo: nombramiento de DPO (cuando sea aplicable); informe de autoría o resultados de las revisiones periódicas efectuadas; análisis de riesgo o evaluaciones de impacto aplicables a sus servicios; modelos de cláusulas utilizadas, políticas de tratamiento de datos, etc.

En los casos en que la actividad del tercero se corresponda con la de un "mero intermediario" que no tendrá acceso a los datos personales, se podría requerir que éste acredite la obtención de evidencias/garantías de cumplimiento similares de aquellas terceras partes cuyos servicios propone al contratante mediante su intermediación.

[10] Por ejemplo, en el sector publicitario es recomendable que los terceros propietarios de tecnologías/soportes hayan implantado un mecanismo acorde al marco de transparencia y consentimiento de la IAB. https://iabeurope.eu/transparency-consent-framework/

[11] https://www.iso.org/committee/45306/x/catalogue/

[12] https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

[13] https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigosde-conducta/codigos-inscritos

7. 3.Recomendaciones durante la contratación con "otros terceros".

Tras haber determinado la naturaleza y alcance de los servicios ofertados, habiendo identificado la condición/rol del tercero en cada fase del tratamiento y evaluado sus garantías de cumplimiento normativo, es preciso formalizar contractualmente la prestación de servicios. En este sentido, se deberán tener en cuenta los resultados obtenidos durante la fase anterior para determinar las obligaciones y responsabilidades atribuibles al tercero y/o las cautelas asociadas a sus servicios. A tales efectos, cabe señalar las siguientes recomendaciones:

- **Establecer contractualmente los tratamientos de datos corresponden a cada parte:** en congruencia con la naturaleza y alcance de los servicios identificada en la fase anterior, es preciso constatar, contractualmente, los tratamientos de datos que se desprenderán de la prestación de servicios. En este sentido, es fundamental estipular pormenorizadamente las diferentes actividades que pudieran concurrir, de acuerdo con el mapa de tratamientos o flujos de datos previsto, estableciendo los distintos "tramos" de tratamientos que pudieran suscitarse para determinar las obligaciones/responsabilidades correspondientes.

  A modo ilustrativo, al establecer contractualmente la relación entre una entidad aseguradora y una correduría, deberían especificarse las actividades/tratamientos/obligaciones que corresponden a cada parte (como "Responsables" separados e independientes). En este sentido, dentro de las prestaciones habituales del corredor, podrían encontrarse: (i) comunicar a la aseguradora los datos personales del tomador, necesarios para formalizar el contrato de seguro; y/o (ii) solicitar, en nombre del tomador, la suscripción de un nuevo contrato o la modificación/rescisión del contrato en vigor.

  En este supuesto, al regularizar contractualmente estas actividades, convendría establecer que el corredor responderá por el cumplimiento del deber de información y de la legitimidad, veracidad y exactitud de los datos derivados del primer "tramo de tratamiento" (comunicación de datos del tomador); y también acreditará haber obtenido el consentimiento del tomador para realizar las acciones que corresponden al "segundo tramo" del tratamiento (modificación/recisión del contrato de seguro). A diferencia de las actividades derivadas del primer "tramo" del tratamiento, la modificación/recisión del contrato de seguro requiere acreditar haber obtenido el consentimiento del tomador.

- **Establecer contractualmente la condición/naturaleza atribuible a cada parte:** es fundamental que el tercero asuma y reconozca, contractualmente, el rol/condición que le corresponde con respecto al tratamiento de datos vinculado al servicio. La granularidad cada actividad/tramo de tratamiento permitirá formalizar el rol que corresponderá al tercero con respecto a cada "prestación" incluida en su servicio. Este ejercicio requiere una especial atención en los supuestos en los que el tercero tiene un rol "ambivalente" (en parte "Responsable" y en parte "Encargado").

  A modo de ejemplo, si los servicios ofertados por un tercero propietario de una App, conllevan a: (i) enriquecer los datos de correo electrónico de los potenciales clientes del contratante a partir de información de la que el tercero dispone, obtenida de los usuarios que, coincidentemente, hayan descargado su "App" utilizando la misma dirección de correo electrónico; y (ii) enviar, en nombre y por cuenta del contratante, distintas comunicaciones comerciales a los titulares de dichos correos electrónicos diferenciadas a partir de la segmentación/perfilado resultante en la primera fase de servicio. En este supuesto, habría que constatar que en el primer "tramo de tratamiento" (enriquecimiento de datos) el tercero actuaría bajo la condición de "Responsable" mientras que en el segundo "tramo" (emailing) actuaría como "Encargado".

- **Establecer contractualmente las responsabilidades de cada parte:** la determinación de las obligaciones y responsabilidades que corresponden a cada parte reviste especial importancia en los supuestos en los que el tercero y el contratante ostentan la condición de "corresponsables del tratamiento" (*Joint Controllers*) . A modo ilustrativo, en el sector sanitario suelen realizarse investigaciones en las que participan varias entidades u organismos. Si, por ejemplo, un centro médico y una residencia de ancianos deciden realizar un estudio sobre los efectos de cierto medicamento suministrado a personas mayores y ambas entidades determinan la finalidad, los medios, el alcance/enfoque de dicha investigación, utilizando datos de sus pacientes/residentes, sería necesario establecer, contractualmente, el "reparto de tareas" e identificar las obligaciones que corresponden a cada parte. A tales efectos convendría constatar, entre otros: (i) a quién correspondería informar y recabar el consentimiento de los pacientes/residentes participantes en el estudio; (ii) quién controlará e implantará las medidas de seguridad aplicables; (iii) cómo se gestionarán las posibles solicitudes de ejercicios individuales; (iv) cuál será el DPO que se designará como punto de contacto para los interesados; (v) quien realizará el análisis de riesgo y/o las evaluaciones

[14] La importancia radica en la mención específica del art. 29 de la LOPDGDD, que a su vez remite al art. 26 del RGPD, que establece: *"Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información…".*

de impacto aplicables al tratamiento previsto; (vi) cómo se gestionarán los posibles incidentes y/o brechas de seguridad.

Finalmente, en un ejercicio de transparencia y responsabilidad proactiva ejercida "conjuntamente", convendría regularizar cómo se establecerán las revisiones periódicas o auditorias que permitan verificar el cumplimiento de las correspondientes responsabilidades (p.e. sometiéndose ambas entidades a una auditoría periódica realizada por un tercero, auditando cada entidad al otro "corresponsable", etc.).

- **Establecer los controles que serán ejecutados posteriormente:** para determinar los controles que habrán de ejecutarse posteriormente, es preciso tener en cuenta los elementos constatados en la fase previa a la contratación, es decir, naturaleza/alcance del servicio, mapa/flujo de datos y prestaciones, condición/rol aplicable a cada fase/tramo del tratamiento previsto y las garantías de cumplimiento normativo acreditadas por el tercero. En este sentido, los controles que se estipulen estarán encaminados a verificar la vigencia y correspondencia de los servicios con respecto a tales elementos constatados. Por ejemplo, se podrán establecer revisiones periódicas cuyo objeto sea confirmar que la naturaleza de los servicios y las actividades derivadas del mismo no han sido modificadas a partir de "nuevos" tratamientos" añadidos durante la vigencia del contrato o ajenos a la descripción de las prestaciones iniciales.

  De la misma manera, si durante la vigencia del contrato se detectan nuevos "tramos de tratamientos" que suponen una modificación a la condición/rol previamente asignado, habría que establecer la posibilidad de reevaluar, en tal circunstancia, si el rol y obligaciones/responsabilidades asignadas al tercero (responsable independiente, corresponsable, "ambivalente", etc.) es congruente con dichas actividades emergentes o si es necesario realizar modificaciones en este sentido.

  Por otra parte, tal y como ocurre en las relaciones con los "terceros habituales" analizados en los apartados anteriores de esta Guía (p.e. con encargados del tratamiento), aquí también sería aplicable que si durante la fase previa se solicitaron certificaciones (ISO 27001, TCF IAB, PCIDSS, etc.), o acreditar la adhesión a normas o códigos sectoriales para comprobar el nivel de cumplimiento y se constató que las mismas estaban próximas a su vencimiento, convendría establecer la obligación de acreditar la renovación posterior o la vigencia continuada

de las mismas para que la validez de tales garantías no resulte "comprometida" durante la prestación del servicio. De igual manera, se podrán requerir nuevos informes de auditoría o nuevas evidencias de cumplimiento (políticas de cookies utilizadas, clausulas de información, muestreo de consentimientos obtenidos, etc.) para comprobar que el grado de madurez del tercero continúa siendo el óptimo.

Aunque la periodicidad y alcance de todos estos controles deberá ser acordada entre las partes, conviene establecer contractualmente los "remedios" que habrán de acometerse para regularizar los "nuevos tratamientos" que puedan detectarse posteriormente, ya sea mediante adenda o instrumento similar, así como las consecuencias derivadas de cualquier incumplimiento, irregularidad o inconsistencia que pueda advertirse a partir de dichas revisiones.

7. 4. Recomendaciones en la fase posterior a la suscripción del contrato con "otros terceros".

Al igual que sucede en la relación con "Encargados del Tratamiento", la obligación de diligencia debida no termina con la firma del contrato que regule la relación y las responsabilidades de cada parte en cuanto al tratamiento de datos personales, sino que debe mantenerse durante todo el ciclo de vida del Tratamiento, también para estos "otros terceros" de los que venimos hablando.

En cuanto a las recomendaciones de control y diligencia, tras la firma del contrato y durante la vigencia del mismo, éstas podrán ser periódicas, con una temporalidad establecida, por ejemplo, en el plan de auditoría de cada compañía en función de: las características de cada tratamiento, del nivel de riesgo detectado y/o de los cambios que puedan producirse en los procesos asociados al mismo. No hay que olvidar que en la relación con "otros terceros" pueden concurrir varios "tramos" de tratamiento de datos, y en cada caso, tanto las obligaciones contractuales como el tipo de relación que se establece pueden diferir y requerir de diferente nivel de control y seguimiento. A continuación, se describen algunas de las recomendaciones, controles y buenas prácticas que podrían aplicarse a la fase posterior a la formalización del contrato:

- **Comprobaciones sobre la vigencia de los servicios y tratamientos de datos inicialmente identificados:** aunque no sea obligatorio, es recomendable para toda empresa tener un Registro de Actividades del Tratamiento (RAT) que sirva de base para conocer no solo los tratamientos que realiza, sino para analizar los

riesgos e identificar a los terceros que participan en cada uno de ellos. Debería existir un proceso de actualización del RAT, ante cambios sustanciales, así como un proceso de revisión periódica para detectar cambios que puedan estar pasando desapercibidos, y que incluya la relación con terceros en cada tratamiento. Esta recomendación se extiende para la relación con cualquier tercero, no solo para los casos objeto de estudio en este apartado.

- **Comprobaciones sobre la condición/naturaleza de las partes:** con la imagen actualizada de las funciones y roles de cada parte, en cada fase del tratamiento, debería comprobarse si la relación establecida sigue siendo la correcta, revisando el análisis que se hizo previamente al establecimiento de la relación contractual. Y de no ser así, deberá modificarse el contrato para adaptarnos a la nueva relación establecida.

  Un ejemplo claro ha sido el cambio de relación entre las empresas de "Gestión de Listados de Solvencia Patrimonial y Crédito" y sus clientes (que establece la LOPDGDD), del que venía existiendo tradicionalmente a la "Corresponsabilidad", que ha debido ser actualizada en todos los casos a un nuevo tipo de contrato y garantías de control.

  Otro ejemplo son las relaciones de socios comerciales o *"parnertship"*, en el que dos empresas llegan a acuerdos de comercialización conjunta de productos de una de ellas, que tradicionalmente se regulaban como "Encargos del Tratamiento" con medidas estándar extraídas de la ley. Si se analiza con casi total probabilidad corresponderán a una relación de *"controller to controller"* o de *"joint controllers to controller"*. En la fase de comercialización del producto los dos socios comerciales podrán decidir los medios y finalidad del tratamiento de datos de los interesados a los que se dirige la venta, pero una vez que se contrata el servicio, únicamente la empresa titular del mismo será la "Responsable" del tratamiento de datos necesarios para su prestación.

- **Modificaciones sobrevenidas:** resulta fundamental revisar las obligaciones y controles establecidos en el contrato y en los procesos internos de control, a tenor del análisis de riesgos actualizado sobre el RAT, y en caso de que sea necesario, actualizar las obligaciones contractuales con cada tercero.

  Se podría realizar comparando los controles que se le asignarían al tercero tras la revisión del análisis de riesgos actualizado y comprobando que están recogi-

dos en el contrato existente. En caso de que no sea así, convendría modificar el contrato para asegurar que todas las medidas y controles necesarios según este análisis de riesgos se han recogido adecuadamente.

- **Ejecución de controles para verificar cumplimiento contractual:** es preciso auditar las obligaciones establecidas en el contrato, lo que podría implicar la revisión de controles y obligaciones tanto propios como del tercero. Cabe advertir que en los casos en que se trate de relaciones más igualitarias no solo existirá una obligación de diligencia y control de nosotros hacia este tercero, sino que lo lógico sería que este tercero también audite al contratante dentro de sus procesos internos. Por lo tanto, convendría generar las evidencias de ejecución de nuestras obligaciones contractuales a la vez que se realiza la auditoría al tercero.

  Cabe reiterar que la relación con "otros terceros" no equivale al típico "Encargo" y que las obligaciones que cada parte asumirá contractualmente con respecto al tratamiento de datos previsto podrían no ser las "estándares". Es probable que utilizar la misma metodología que la empleada para "Encargados", sin adaptar, no resulte lo más adecuado. Por tanto, lo recomendable sería estudiar cada tipo de relación para ver si encaja mejor en la metodología y procedimientos de control y auditoría a "Encargados" o en los de auditorías propias internas.

  A modo ilustrativo, en una relación de *"controller to controller"* puede que la obligación de información al interesado recaiga en uno de los intervinientes pero que el contenido de dicha información sea definido y decidido por ambas partes. Por ejemplo, si una empresa capta datos de usuarios potenciales clientes "leads" en Internet y obtiene su consentimiento para comunicar dichos datos a otra empresa para utilizarlos en sus procesos internos de venta, el deber de informar y recabar el consentimiento será exclusivo de la primera empresa, pero el contenido de la información a facilitar puede ser acordado entre ambas partes. En este supuesto, la auditoría podría suponer: (i) comprobar que el contenido de la información facilitada a los usuarios/leads se mantiene actualizada y conforme al tratamiento; (ii) obtener evidencias de que se está informando adecuadamente a los usuarios y obteniendo su consentimiento.

  En el caso del primer control (contenido de la información) puede realizarse de forma conjunta entre ambas partes, mientras que el segundo (evidencias) podría formar parte del proceso de auditoría a terceros, o podría realizarse como un anexo al proceso de auditoría interna por su mayor relación con los procesos internos de auditoría.

Adicionalmente, pueden presentarse situaciones en las que la auditoría no es ni interna ni a la tercera parte "stricto sensu". Por ejemplo, en una "Corresponsabilidad" del tratamiento en la que ciertos medios técnicos, como un Sistema de Información, es mantenido de forma conjunta por ambas partes. En estos casos, a priori parece que tenga más sentido realizar el control dentro del proceso de auditoría interno, puesto que habrá muchos elementos de la propia compañía a comprobar y que además serán comunes a otros Sistemas Internos (p.e. procedimientos, control de accesos, pasos a producción, etc.), pero el análisis se complementaría con el control que le correspondería ejecutar a la "otra parte" corresponsable.

- **Ejecución de enmiendas:** todo plan de control y auditoría debe llevar aparejado un plan de mejora continua, es decir, que ante los incumplimientos detectados será necesario establecer un plan de acción para que se subsanen. A diferencia de un "Encargo" en los que cabría recordarle al tercero sus obligaciones contractuales y conminarle a ejecutarlas correctamente, cuando se trata de "otros terceros", este plan de acción conllevaría a reevaluar la relación, los acuerdos y establecer nuevos controles y obligaciones para cada parte.

Por último, dentro de la fase posterior a la suscripción del contrato se encuentran las provisiones aplicables al fin de la relación que se ejecutarían conforme a lo establecido contractualmente. En estos casos, ya no se trataría simplemente de destruir o devolver la información como en el caso de un "Encargado", sino que habría que advertir circunstancias en las que el fin de la relación venga marcado por el fin del tratamiento o por su modificación sustancial. Y en este caso nuestra responsabilidad sería la de verificar que tanto nosotros como los "otros terceros" proceden conforme a la normativa aplicable durante la finalización del contrato.

08

Conclusiones

En este capítulo se recogen a modo de resumen los aspectos más relevantes de lo visto a lo largo de la Guía, de forma que pueda servir incluso para, de un vistazo, entender el enfoque de gestión propuesto en los capítulos anteriores.

Según se exponía en la introducción, se ha presentado una propuesta de cómo abordar de manera la práctica la gestión del riesgo de terceros en el ámbito de la privacidad; como también se ha indicado, se ciñe el concepto de "tercero" al de "encargado del tratamiento", definido en el artículo 4.8 RGPD como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

Las funciones que desarrolla el encargado serán realizadas por cuenta del responsable, de forma que será éste y no el encargado el que tome las decisiones en relación con los elementos esenciales del tratamiento (fines y medios del tratamiento).

El artículo 28 del RGPD obliga al responsable a elegir únicamente a aquellos encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de tal manera que el tratamiento que realicen por cuenta del responsable sea conforme con los requisitos establecidos en la citada normativa.

Precepto que encuentra su justificación en el art. 5.2. RGPD que recoge el principio básico de la "responsabilidad proactiva" o *accountability*, tradicionalmente conocido también como "obligación de diligencia debida".

En consecuencia, el RGPD da un paso más en su enfoque de riesgos y exige una mayor responsabilidad y control a los responsables y encargados; no solamente en el momento meramente contractual sino también a en los momentos anteriores y posteriores a la firma del contrato, e incluso en el momento de la terminación de dicha relación o prestación de servicios.

Por esta razón, antes de compartir datos de carácter personal con terceros las organizaciones (responsables del tratamiento) deben llevara a cabo una evaluación de riesgo de los mismos.

Dicha evaluación deberá comprender las siguientes fases:

- Identificación de todos los proveedores que vayan a tratar datos personales por cuenta de nuestra organización.

- Análisis de la tipología de los datos que van a ser tratados.
- Análisis de la situación contractual con dicho proveedor.
- Preparación de la evaluación y requisitos de cumplimiento normativo.

Asimismo, se considera también una fase de homologación, o de identificación de aquellos candidatos a ser proveedores, para verificar si están en condiciones de ofrecer en el futuro las garantías de gestión de datos que demanda nuestra organización.

La protección de datos se convierte así, en otro elemento fundamental, previo a la selección del proveedor, junto con las ya tradicionales cuestiones de negocio, financieras o logísticas.

Se deben solicitar garantías de cumplimiento previas a la contratación y, una vez seleccionado el tercero, el contrato debe contener, con claridad, determinados elementos esenciales, esto es, los tratamientos de datos que realiza cada parte en cada fase y en qué concepto o rol los realiza. Con ello quedará más fácilmente identificada el régimen de responsabilidad que asume cada parte. Igualmente, otro elemento fundamental del contrato serán las garantías de cumplimiento normativo acreditadas por el tercero. Finalmente, deberá quedar perfectamente regulado en el contrato, los controles que serán ejecutados posteriormente, encaminados a verificar la vigencia y correspondencia de los servicios con respecto a tales elementos constatados.

La no formalización del contrato de encargo de tratamiento de datos es infracción de la normativa de protección de datos. En España está tipificada en la nueva LOPDGDD como infracciones graves o muy graves según los artículos 73 y 74.

El contrato de protección de datos no solo da cumplimiento a la normativa en cuestión, además es una forma de definir las responsabilidades entre las partes. Por otro lado, su complimiento beneficia la formalización de acuerdos y responsabilidades de las partes, y es un punto de agarre y defensa entre las mismas.

En todos los supuestos se han de incluir aspectos concretos relacionados con la finalización del contrato, cobrando especial relevancia los mecanismos que se hayan establecido para la devolución o destrucción de la información en esta fase de finalización del servicio.

Para ello, es muy relevante la colaboración con las áreas de negocio que han contratado la prestación de servicios, de cara a poder determinar en qué casos será más con-

veniente ejecutar el contenido de las cláusulas de resolución del contrato y resolver anticipadamente el mismo, o en cuáles se deberá articular una solución de otra índole, mediante lo indicado en los controles internos para la subsanación del incumplimiento por parte del encargado y la monitorización de la evolución por parte del responsable.

Finalmente, puede suceder que la relación con el tercero no sea una relación responsable a encargado. Puede suceder que estemos ante "comunicaciones de datos" donde las terceras partes adquieren el rol de responsables o, en general "otros terceros" que no son típicos "encargados" de los que se pueda "requerir" ciertas "garantías estandarizadas" por imperativo legal, sino que se trataría de *partners* cuya posición contractual podría ser más "equitativa" o de entidades que tratan datos bajo sus propias finalidades y disponiendo de sus propios medios. Por tanto, nuestro análisis no podría derivar en un "requerimiento estándar" (tipo *checklist*) aplicable a todas las contrataciones sino en un verdadero ejercicio de "debida diligencia", considerando, en cada caso, los elementos particulares de la naturaleza/alcance del servicio, mapa/flujo de datos y prestaciones, condición/rol del tercero en cada fase/tramo del tratamiento previsto. Al ser la corresponsabilidad una figura nueva en el marco legal español, es imprescindible un cuidadoso análisis a fin de identificar los supuestos en los que esta aparece.

Debe quedar todo perfectamente documentado a fin de poder acreditar en todo momento tanto la debida diligencia del Responsable del Tratamiento como las decisiones y actuaciones llevadas a cabo.

09

Anexos


SECURITY
REGULATIONS
INSPECTION
IN COMPLIANCE
IN COMPLIANCE
APPROVAL

9.1. Anexo I - Otras regulaciones y buenas prácticas

9.1.1. Otras regulaciones

Entorno ISO

A menudo, el entorno de cumplimiento general del propio RGPD debe completarse, por motivos sectoriales o de negocio, con el cumplimiento o la adopción de determinados estándares. Aunque no existe una exigencia estrictamente legal para su adopción, son muchas las empresas que deciden acudir a dichos estándares, lo que también nos ayuda a entender y comprender que es realmente la "diligencia debida" exigida por el legislador del RGPD.

No estamos refiriendo, por ejemplo, a la Norma de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS), u otros marcos de referencia (Swift, eIDAS, Sepa, etc. para el sector financiero, guías de UNESPA para el sector asegurador, o NIST, SOC, etc. para el resto).

También podría ser el caso de algunos estándares reconocidos y utilizado por multitud de empresas como:

- ISO 37000 Sistemas de Gestión antisoborno e ISO 19600 Sistemas de Gestión de *Compliance* Penal. En ambos casos los controles para cubrir los riesgos relacionados con terceros, denominados socios de negocio, no cubren riesgos relacionados con la protección de datos, pero sí que obligan a la existencia de una metodología de gestión de estos socios que cubra las tres fases de la relación: selección, formalización y seguimiento dentro de la diligencia debida en la que se basan también ambos estándares. Tato por sinergias como por tener una base de partida sobre la implantación de la diligencia en estas fases, estas ISOs pueden servir de base a la hora de definir los controles de diligencia en materia de protección de datos dentro de un plan de *Compliance* más amplio en la organización.

- ISO 27000 incluye un apartado completo de gestión de proveedores en el que se establecen controles efectivos para realizar una gestión de la seguridad de la información en la relación con proveedores: se trata de tres controles en el apartado de selección del proveedor y otros dos en el apartado de provisión, que son una base sólida para establecer los controles internos en la fase precontractual,

de servicio y a su finalización.

- ISO 27701, que se configura como una extensión de la 27001 para poderse beneficiar de los estándares de seguridad, pero que incluye requisitos específicos para la gestión de datos personales; y en concreto, dos anexos de objetivos de control (condiciones de recogida de datos personales, obligaciones principales, *privacy by design*, o transferencias internacionales) y controles específicos dirigidos tanto a responsables como a encargados y que ayudaran a marcar una pauta sobre que podemos entender por diligencia debida.

Esquema Nacional de Seguridad

Por otro lado, esa obligación de diligencia debida también es exigida, más allá de la normativa general RGPD y estándares de aplicación, en sectores o ámbitos concretos, con normativas particulares y específicas como podría ser el caso del sector público (ENS), el sector bancario, el sector de las telecomunicaciones, el sector asegurador, las infraestructuras críticas, etc.

Banca

Por ejemplo, en el sector bancario, la Guía EBA/GL/2019/02 de 25 de febrero del 2019 que establece las Directrices de Externalización y las recomendaciones EBA/REC/2017/03 de 28 de marzo del 2018 sobre externalización de servicios en la nube; establecen a obligación de las entidades financieras de analizar los todos los riesgos que conlleva la externalización de servicios, debiendo categorizarlos en servicios "críticos" y "no críticos" así como analizar y proteger la confidencialidad y seguridad de la información a la que acceden. En el mismo sentido, la Norma 43 de la Circular 2/2016 de 2 de febrero del Banco de España, sobre "Delegación de la prestación de servicios o del ejercicio de funciones" señala que las entidades de crédito a la hora de contratar a un proveedor deberán tener en consideración, entre otras cuestiones, el riesgo de incumplimiento de las normas.

Infraestructuras Críticas

En el sector de las infraestructuras críticas, El 7 de septiembre entró en vigor el Real Decreto Ley 12/2018, de Seguridad de las Redes y Sistemas de Información (que transpone la Directiva NIS (UE) 2016/1148, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de

información en la Unión) y que resulta aplicable a los operadores de servicios esenciales, entre los que se encuentra la práctica totalidad de los designados como operadores de infraestructuras críticas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC) (además de a los prestadores esenciales de un *servicio digital*- mercados en línea, motores de búsqueda en línea y servicios de computación en nube-, siempre que no sean pymes o micropymes); estableciendo, entre otras obligaciones, la de adoptar medidas técnicas y de organización, o la de notificar incidentes tanto propios como de los proveedores. En este sentido, la "Guía nacional de notificación y gestión de ciberincidentes" del Consejo de Ciberseguridad Nacional de 9 de marzo de 2019 -aplicable tanto a sector público como privado-; establece una previsión específica dirigida a los proveedores de los operadores de infraestructuras críticas señalando que *"Asimismo,* ***aquellos proveedores de los sujetos obligados por este anexo que proporcionen sus productos o servicios a éstos, y cuyas actividades tengan afección directa a la prestación de un Servicio Esencial, deberán cumplir con los mismos criterios exigibles a los operadores****. En todo caso, el operador afectado será el responsable último del cumplimiento de los requerimientos exigibles en este texto"*.

Vemos por tanto, que en cuanto a la gestión de terceras partes en relaciones mercantiles de prestación de servicios que implique acceso a datos personales o a información confidencial en general de una organización, la relación Responsable de la Información – Proveedor de servicios está incluida en muchos estándares y legislación que obliga a un control diligente por parte del Responsable y que incluye una serie de obligaciones de control y diligencia en las diferentes fases de la relación: pre, contractual y postcontractual, más allá del Reglamento General de Protección de Datos. Es el caso, por ejemplo, del Esquema Nacional de Seguridad: con rango de ley y obligatoria para todas las Administraciones Públicas incluye entre sus requisitos mínimos la obligación de la AAPP de verificar que todo producto que adquiera o contrate cumpla con todos los requisitos del ENS, debiendo valorarse positivamente las certificaciones en cuanto a seguridad que aporte. Además, las medidas de seguridad obligatorias para toda la información tratada un apartado de Servicios Externos, que incluye la contratación, la gestión diaria y los medios alternativos.

Dado que cualquier proveedor de las AAPP españolas está obligado a cumplir con el ENS, incluir entre las obligaciones internas a cumplir las de diligencia y gestión de terceras partes, siguiendo las directrices del ENS, puede simplificar procesos internos y dar luz a tareas y medidas a implantar en el proceso de diligencia en la gestión de terceros.

9.1.2. Buenas prácticas

Pero además del RGPD, existen otras normas y estándares, como las indicadas en el apartado "otras regulaciones", que imponen a los responsables otras obligaciones como:

Disponer de una política de externalización aprobada por su Consejo de Administración, en la que se definan los principios que deben regir en la externalización de servicios.	Nombrar a un órgano cuya función principal sea garantizar que se cumple la política y que se analizan todos los riesgos derivados de la externalización.
Definir un marco de control que evalúe los riesgos derivados de la externalización (riesgo de incumplimiento legal, riesgo de concentración derivado de la acumulación de servicios y funciones delegadas en un mismo proveedor, riesgo inherente al país al que está ubicado el proveedor, riesgo reputacional derivado de las practicas seguidas por el proveedor).	La valoración en la elección del proveedor del grado en que este cumple con las leyes y normas más relevantes que le son de aplicación.
Evaluación y gestión de conflictos de interés.	Nombramiento de un representante dentro de la Unión Europea.

Se podría considerar una buena práctica que todas las organizaciones dentro de su marco normativo interno incluyan una política de externalización en la que se determinen claramente los principios que deben regir en la externalización de servicios, cuenten un procedimiento de homologación de proveedores para garantizar que se cumple con todos los requisitos legales, se definan la periodicidad de las auditorias, cuente con un código de conducta específico para proveedores o qué documentación debe aportar el proveedor para cumplir con el principio de diligencia en la elección y por tanto demostrar que se ha elegido a un proveedor que ofrecía garantías suficientes.

9.2. Anexo II - Anexos a incluir en un contrato de encargo de tratamiento

Según se indicó en el capítulo 3.2 FASE CONTRACTUAL, el CET puede acompañarse de diversos anexos. Entre ellos un cuadro identificativo del tratamiento, tipología de datos, finalidad del tratamiento y categoría de los interesados; y la relación de las empresas subcontratadas por el encargado de tratamiento, conteniendo el nombre de la entidad, la actividad subcontratada, ubicación y garantías implementadas. Se ofrece a continuación un ejemplo de la estructura que podrían tener dichos anexos al CET.

9.2.1. Datos objeto de tratamiento

OBJETO	
TRATAMIENTO A REALIZAR	Recogida. Registro. Estructuración. Modificación. Conservación. Extracción. Consulta. Comunicación por transmisión. Difusión. Interconexión. Cotejo. Limitación. Supresión. Destrucción. Comunicación. Otros:
FINALIDAD DEL TRATAMIENTO	Gestión de clientes, contable, fiscal y administrativa. Gestión de nóminas. Prestación de servicios de solvencia patrimonial y crédito. Servicios económico-financieros y de seguros. Publicidad y prospección comercial.

OBJETO	
FINALIDAD DEL TRATAMIENTO	Guías/repertorios de servicios de comunicaciones electrónicas. Prestación de servicios de certificación electrónica. Gestión de actividades asociativas, culturales, recreativas, deportivas y social. Educación. Gestión y control sanitario. Seguridad privada. Videovigilancia. Recursos humanos. Prevención de riesgos laborales. Cumplimiento/incumplimiento de obligaciones dinerarias. Análisis de perfiles. Prestación de servicios de comunicaciones electrónicas. Comercio electrónico. Gestión de asociados o miembros de partidos políticos, sindicatos, iglesias. Gestión de asistencia social. Investigación epidemiológica y actividades análogas. Historial clínico. Seguridad y control de acceso a edificios. Fines estadísticos, históricos o científicos. Otros:
TIPO DE DATOS	Datos de carácter. identificativo. Características personales. Académicos y profesionales. Información comercial. Circunstancias sociales. Detalles del empleo. Económicos, financieros o de seguros información comercial.

OBJETO	
TIPO DE DATOS	Transacciones de bienes o servicios. Categorías especiales de datos. Otros:
CATEGORÍAS DE INTERESADOS	Empleados. Clientes y usuarios. Proveedores. Asociados o miembros. Propietarios o arrendatarios. Pacientes. Estudiantes. Personas de contacto. Padres o tutores. Representante legal. Solicitantes. Beneficiarios. Cargos públicos. Otros:

9.2.2. Empresas subcontratistas

Nombre de la entidad	Actividad de tratamiento	Ubicación	Garantía adecuada implementada

9.3. Anexo III - Checklists para el control de las fases en la contratación

Como se ha podido ver en el desarrollo de la Guía, se definen una serie de fases en la gestión de riesgos de terceros en el ámbito de la privacidad. El presente anexo incluye una serie de *checklists* orientativas que permitan a los responsables de las fases correspondientes controlar que se han tenido en cuenta, en cada una de ellas, todos los aspectos relevantes, según la propuesta del presente documento.

Como se verá, el mismo requerimiento o punto de control se puede incluir en más de una *checklist*, lo que obedece a que el enfoque y alcance efectivo puede ser distinto en función de la fase en que se está haciendo. Por otro lado, al ser orientativas, en la aplicación práctica se pueden seleccionar las cuestiones necesarias para cubrir todo el espectro sin repetir revisiones innecesariamente.

A la hora de gestionar las *checklists*, téngase en cuenta que aquellas preguntas contestadas por un NO pueden señalar carencias en el cumplimiento con las normas por parte de terceros o debilidades en nuestro proceso. En esos casos, se recomienda una lectura detallada del capítulo de referencia de la presente Guía.

9.3.1. Checklist para la Fase de homologación

El artículo 5.2 del RGPD recoge el principio de "responsabilidad proactiva" o *accountability*, lo que lleva directamente a que el responsable deba ejercer un plus de control sobre la gestión del proveedor o tercero en general, demostrando en todo caso su proactividad[15].

Esta necesaria proactividad se extiende más allá del proveedor que contrata o colabora con el responsable, alcanza (consecuentemente con el principio de *accountability*) a aquellos terceros que pretenden mantener en el futuro esa relación de proveedor o colaborador. Así, el artículo 81 RGPD señala que el responsable (…) debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.

Por tanto, a diferencia del régimen normativo anterior, basado exclusivamente en un cumplimiento meramente formal y/o contractual, el RGPD da un paso más en su en-

[15] Pto. 1 de la Guía: Regulación de la Obligación de Diligencia Debida.

foque de riesgos y exige una mayor responsabilidad y control a los responsables y encargados; no solamente en el momento meramente contractual sino también a en los momentos anteriores y posteriores a la firma del contrato, e incluso en el momento de la terminación de dicha relación o prestación de servicios.

En la misma línea, las "Directrices para la elaboración de contratos entre responsables y encargados de tratamiento" elaboradas por la AEPD, APDCAT y AVPD señalan que *"el RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD. Y ello, implica la necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD"*.

Lo que lleva a que la valoración del cumplimiento de los proveedores, encargados del tratamiento, debe realizarse con carácter previo y anticipado a la puesta en marcha del correspondiente tratamiento o prestación de servicios por parte del proveedor.

Así, con carácter previo a la contratación, en el proceso de homologación, deberá constatarse[16]:

- Que en el uso de la información personal se respeta lo establecido en el artículo 5.2 del RGPD (responsabilidad proactiva); es decir, verificar que cumple con lo previsto en el RGPD.

- Que el aspirante a proveedor ha adoptado las medidas de seguridad, técnicas y organizativas previstas en el artículo 32 del RGPD.

- Que cuenta con mecanismos para verificar esas medidas (art. 24.1).
  Que cuenta con políticas y procedimientos que garanticen que aplica medidas de seguridad desde el diseño. (art. 25).

- Que cuenta con un registro de actividades de tratamiento, en los casos en que sea necesario (Art. 30).

- Que cuenta, en los casos exigidos, con un Delegado de Protección de Datos (Art. 37-39).

- Que garantiza, mediante el procedimiento adecuado, que se van a notificar y co-

[16] Pto. 1.1. Cumplimiento.

municar las brechas de seguridad que pudieran producirse (Art. 33 y 34).
Que se han llevado a cabo los pertinentes análisis de riesgos y evaluaciones de impacto (Art. 35).

- Que se realizan o no transferencias internacionales de datos (Art. 44).

Por otra parte, aunque no exista exigencia legal, el hecho de que el proveedor disponga de certificaciones de seguridad contrastadas y adopte estándares admitidos, puede ser indicativo para demostrar un determinado grado de gestión de la seguridad de la información. Este hecho debe llevar a considerarlo en el proceso de homologación.

A continuación, se ofrece una propuesta de los puntos que habría que incluir en la lista de comprobación o cuestionario para la homologación de los proveedores en el ámbito de la privacidad. En los apartados siguientes, como se ha dicho, se ofrecen los correspondientes cuestionarios para las restantes fases del proceso, bajo la misma perspectiva:

	Pregunta	Sí	No
1	¿Garantiza que cumple con las directrices del RGPD, y, en consecuencia, adopta las medidas de seguridad que establece?		
2	¿Tiene política de seguridad de la información y privacidad?		
3	¿Se ha sometido a auditoría de privacidad o protección de datos en los últimos dos años?		
4	¿Realiza los pertinentes análisis de riesgo y evaluaciones de impacto?		
5	¿Tiene un procedimiento para tratar y comunicar las posibles brechas de seguridad?		
6	¿Dispone de DPO? (Caso de que sea necesario)		
7	Dispone de protocolo para tratar todo tipo de incidencias de seguridad		
8	Si es necesario, ¿cuenta con un registro de actividades de tratamiento?		

	Pregunta	Sí	No
9	¿Asume, mediante su firma, las cláusulas de confidencialidad e instruye a sus empleados sobre las mismas y a la debida confidencialidad que tienen que observar con los datos personales que tratan?		
10	Indique las principales certificaciones o estándares que posee la Compañía en materia de seguridad de la información (ISO 27001, ISO-25999,…) (Indique certificación, entidad certificadora, y fecha de certificación)		
11	¿Aplica medios para detectar vulnerabilidades tecnológicas y procesos para corregirlas?		
12	¿Subcontrata a terceros para llevar a cabo la prestación de sus servicios?		
13	Si subcontrata con terceros, ¿les comunica las cláusulas/exige las medidas de seguridad requeridas?		
14	¿Disponen de un Plan de Continuidad de Negocio?		

9.3.2. Checklist para la Fase Precontractual

	Pregunta	Sí	No
1	¿Está el tercero en posesión de un certificado de protección de datos?		
2	En su caso, ¿se ha verificado el nombramiento de DPO y su registro ante la autoridad de control competente?		
3	¿Se van a llevar a cabo Transferencias Internacionales de Datos en el ámbito del contrato?		
4	En tal caso, ¿se ha confirmado la existencia de garantías adecuadas para llevarla a cabo de acuerdo con la regulación?		
5	¿Se ha verificado la llevanza de un Registro de Actividades de Tratamiento?		

	Pregunta	Sí	No
6	¿Cuenta el tercero con Políticas de protección de datos personales, tiene implantados los avisos de privacidad así como un proceso de gestión de solicitudes de ejercicios de derechos, incidentes, reclamaciones etc.?		
7	Si el tercero fuera un encargado, ¿se ha verificado la existencia de posibles subcontrataciones (subencargados del tratamiento y los correspondientes acuerdos de protección de datos con terceros)?		
8	¿Existe algún procedimiento sancionador o de investigación y/o sanciones al encargado del tratamiento en materia de protección de datos al menos, de los últimos 5 años?		
9	¿Se ha comprobado la existencia de medidas de seguridad implementadas y el cumplimiento de los requisitos del RGPD, como por ejemplo los mecanismos para el ejercicio de derechos?		
10	¿Se ha verificado que dispone de un Procedimiento o protocolo de gestión de brechas de seguridad?		

9.3.3. Checklist para la Fase Contractual

	Pregunta	Sí	No
1	¿Se han identificado obligaciones específicas contiene el RGPD para los encargados de tratamiento?		
2	¿Se ha procedido a acreditar la existencia de garantías suficientes del encargado de tratamiento?		
3	¿Se ha verificado que el contrato de encargo de tratamiento contiene todo lo prescrito por el RGPD?		

	Pregunta	Sí	No
4	Si el contrato con el encargado del tratamiento fuera anterior al RGPD, ¿se ha confirmado su validez?		
5	Si se realizaran transferencias internacionales de datos para la prestación del servicio, ¿se ha verificado la existencia de un mecanismo válido para llevarlas a cabo?		
6	En caso de que el tercero no sea un encargado, ¿se han identificado igualmente las obligaciones impuestas por el RGPD en su caso y que estas se han incluido en el contrato?		

9.3.4. Checklist para la Fase Poscontractual

	Pregunta	Sí	No
1	¿Se han tenido en cuenta aspectos concretos relacionados con la Finalización del Contrato?		
2	¿Se ha valorado del nivel de riesgo de proveedor o incluso del impacto que pueda tener el servicio en la continuidad del negocio de la entidad específicamente a la finalización del contrato?		
3	¿Se ha confirmado que los aspectos concretos relacionados con la finalización del contrato se ajustan al nivel de riesgo del proveedor o al impacto que el servicio puede tener en la continuidad del negocio al llegar el contrato a término?		
4	¿Se va a producir un traspaso de los datos personales a un nuevo proveedor?		

	Pregunta	Sí	No
5	En caso de que se produzca el traspaso de los datos personales, ¿se han adoptados las medidas de seguridad adecuadas para que este se produzca sin incidencias o brechas?		
6	¿Se han establecido mecanismos para la devolución o destrucción de la información en esta fase de finalización del servicio?		
7	En caso positivo, ¿se ha verificado que la supresión de los datos personales se realizará de manera segura llegado el caso? (por ejemplo, solicitando un certificado de destrucción)		
8	¿Se ha incluido expresamente la posibilidad de finalización del servicio en el caso de que se infrinjan las disposiciones legales, regulatorias o contractuales aplicables o cuando existan deficiencias en la gestión y la seguridad de los datos de carácter personal o confidenciales en el propio contrato?		
9	¿Se ha valorado la responsabilidad legal asociada al proveedor en caso de incumplimiento?		
10	¿Se ha considerado un potencial reparto de culpas?		
11	¿Se ha valorado la posibilidad de que exista exención de responsabilidad de alguna de las partes en caso de que se pudieran haber causado daños durante o a la finalización de la relación contractual?		
12	Llegado el caso, ¿se han adoptado medidas a fin de evitar que el proveedor pueda eludir su responsabilidad frente a los afectados?		
13	¿Se ha asegurado que el proveedor transferirá el conocimiento adquirido o generado durante la prestación del servicio a la organización o al proveedor que ésta designe a la finalización del servicio?		
14	¿Se ha asegurado que el proveedor transferirá la documentación adquirida o generada durante la prestación del servicio a la organización o al proveedor que ésta designe a la finalización del servicio?		

	Pregunta	Sí	No
15	¿Se ha asegurado que el deber de confidencialidad del proveedor se mantiene incluso una vez finalizada la relación contractual?		
16	¿Se han eliminado los permisos, tanto físicos como telemáticos, de acceso del proveedor?		

9.3.5. Controles y garantías adicionales en el caso de finalización del contrato por incumplimiento

	Pregunta	Sí	No
1	Antes de comenzar con todos los trámites, ¿se ha revisado el contrato a fin de confirmar si contenía disposición relativas a la terminación y si se regulaba de algún modo la forma o los motivos por los que se puede terminar el contrato?		
2	¿Se han identificado y documentado los incumplimientos que se han producido por parte del proveedor y que derivan en la finalización del contrato?		
3	¿Se ha realizado el aviso por escrito para cualquier tipo de terminación?		
4	¿Se ha asegurado que el proveedor transferirá el conocimiento adquirido o generado durante la prestación del servicio a la organización o al proveedor que ésta designe a la finalización del servicio?		
5	¿Se ha asegurado que el proveedor transferirá la documentación adquirida o generada durante la prestación del servicio a la organización o al proveedor que ésta designe a la finalización del servicio?		
6	¿Se ha asegurado que el deber de confidencialidad del proveedor se mantiene incluso una vez finalizada la relación contractual?		

	Pregunta	Sí	No
7	¿Se han eliminado los permisos, tanto físicos como telemáticos, de acceso del proveedor?		
8	¿Se está trabajando en colaboración con las áreas de negocio que han contratado la prestación de servicios a fin de poder determinar cómo ejecutar el contenido de las cláusulas de resolución del contrato y poder identificar el impacto potencial en el procesamiento de los datos personales?		
9	¿Se ha documentado oportunamente tanto la debida diligencia del Responsable del Tratamiento como las decisiones y actuaciones llevadas a cabo a fin de poder acreditarse en todo momento?		

9.3.6. Controles y garantías adicionales asociados a la finalización del contrato de proveedores estratégicos o de riesgo alto

	Pregunta	Sí	No
1	¿Se cuenta con una garantía de la devolución de los datos o supresión de los mismos por parte del tercero?		
2	¿Se cuenta con una garantía del borrado de las copias de seguridad por parte del tercero?		
3	¿Se ha llevado a cabo un análisis de todos los accesos (VPN, enlaces de comunicaciones, accesos físicos por parte del personal, etc.), usuarios y permisos creados para tal fin a fin de identificar todas las acciones que puedan ser necesario para garantizar la eliminación de todos esos permisos?		
4	¿Se ha identificado el material de la empresa cedido al proveedor para la prestación del servicio y control sobre la devolución de los mismos?		
5	¿Se ha analizado el control de los accesos de la empresa a los entornos y sistemas del proveedor?		

9.4. Anexo IV - Gestión de riesgos

Es objeto de este anexo establecer un paralelismo con un proceso clásico de gestión de riesgos. Para facilitar su lectura independiente, se sigue todo el proceso de gestión de terceros visto en el cuerpo de la presente Guía.

Tendríamos que partir de una fase preliminar para identificar los riesgos que podrían afectar a los activos de nuestro alcance; es decir, hablaríamos de la elaboración del mapa de riesgos y activos. A continuación, en ese hipotético proceso de gestión de riesgos, se debería proceder a identificar los riesgos que realmente están presentes en nuestros procesos, nos referimos a identificarlos mediante métodos racionales y estandarizados, una vez centrados los riesgos que afectan a estos activos de nuestra organización, procederíamos a su análisis y evaluación; es decir, pondríamos el foco en las causas concretas y en cómo nos afectan, en el daño o impacto que podrían ocasionarnos. Una correcta evaluación, cualitativa o cuantitativa, contribuiría de manera decisiva a establecer la prioridad de nuestras actuaciones para tratar esos riesgos. Con esto último entraríamos en las medidas correctivas para eliminar las situaciones de riesgo o minimizar sus efectos, o en un paso más allá, abarcando todo el espectro del tratamiento, podríamos contemplar la posibilidad de transferir el riesgo (mediante el aseguramiento clásico) o de asumirlo, amabas opciones referidas a la totalidad del riesgo o a su carácter residual como complemento a las medidas adoptadas.

Aplicando estas fases al proceso de gestión del riesgo de privacidad en terceros (admitiendo un concepto amplio en el que se engloba cualquier relación con ajenos a la compañía, diferente de la clientelar, mediante el que se pone de algún modo a su disposición o en su conocimiento, datos personales de los que la propia organización es responsable), tendríamos las siguientes fases como conjunto de actuaciones necesarias:

1. Elaboración del mapa de riesgos y activos.

La organización debe elaborar el mapa de riesgos (RTO). Deberá controlar los datos personales que un tercero procesa[17] para el responsable al proveerle de un bien o un servicio. En esta misma línea, distinguirá la calidad del tercero (encargado, responsable u otro) en orden a su relación con la organización que motiva el acceso a esos datos.

Es decir, en esta fase deberá determinar el mapa/flujo del tratamiento de dato, estableciendo un mapa exhaustivo de las actividades que serán realizadas que incluya, entre otros, los tipos de datos utilizados y los flujos de información e intervenciones de cada

[17] Entiéndase procesar aquí según la definición de tratamiento de datos personales en el artículo 4.2) RGPD.

parte para determinar la naturaleza y condición de las partes implicadas, estableciendo el rol o condición atribuible al tercero, ya sea durante el servicio o en cada una de las fases/tramos de su prestación.

En cuanto a la identificación de riesgos potenciales, se englobarían todos bajo el epígrafe "Riesgo de Privacidad", y, si se profundiza en el mismo, especificando para cada tipo de tercero los posibles incumplimientos del RGPD.

2. Homologación

El proceso de homologación no forma parte de forma estricta del proceso de contratación, porque el hecho de que un tercero esté homologado como proveedor o colaborador de nuestra organización, no implica que llegue a formalizar ese contrato; simplemente, indica que cumple los requisitos mínimos para alcanzar ese nivel de relación. Pero no deja de ser cierto que la organización debe marcar las pautas para que, a priori, estos terceros tengan esa posibilidad de contratar o colaborar con nuestra organización.

Es evidente que esta acción opera como un filtro y un sistema de prevención, puesto que llevará a descartar de la relación contractual al tercero que no cumpla esos requisitos, o, al menos, a marcar los que deberá obtener caso de que en el futuro pueda ser contratado.

En este sentido, la organización deberá marcar los requisitos de gestión del riesgo de privacidad (aparte de otros de índole administrativa, reputacional, financiera, etc.) sin los cuales no podrá contratar o colaborar con nuestra entidad. Entre estos requisitos se marcarán los que descartarían cualquier tipo de relación con este tercero y los que la permitirían si se subsanan.

3. Fase de contratación

Dentro de la fase de contratación es necesario distinguir unas subfases en aras a marcar con mayor precisión las acciones necesarias para gestionar el riesgo de privacidad derivado de la acción de terceros.

El contrato se iniciará con la licitación del servicio, continuará con la formalización y resolución del concurso, para llegar a la contratación del concursante que resulte adjudicatario.

3.1. Licitación

La organización apreciará la necesidad de contar con determinado servicio. Desde el momento de su diseño, deberán mapearse los posibles riesgos potenciales del mismo e cuanto a la privacidad y los requerimientos del posible prestador del servicio para minimizarlos. Para esta labor es importante contar con el RTO que se mencionaba como acción preliminar de la gestión de este riesgo.

Hay que destacar que, hasta esta fase, por razones obvias, no es posible identificar o concretar los riesgos de un servicio concreto (salvo que se trate de gestionarlo en contratos que ya se están desarrollando).

Con la selección de posibles prestadores del servicio, de entre los terceros homologados, se estará en condiciones de analizar los potenciales riesgos que cada uno de ellos pudieran presentar

Esta fase requiere un análisis y valoración de los riesgos de privacidad: los posibles derivados de la prestación de este servicio, aquellos conocidos por los posibles prestadores, qué requerimientos o salvaguardas deben adoptarse para eliminarlos; o en su caso, si tienen capacidad para minimizarlos o no. Es recomendable que la licitación se materialice con un pliego en el que ya se marquen las condiciones de seguridad, certificaciones y clausulados de confidencialidad, etc., a los que debe adherirse el futuro proveedor o colaborador, etc.

3.2. Concurso

Se menciona el proceso del concurso, como la deliberación para elegir al proveedor o tercero que prestará el servicio de entre los concurrentes al proceso. La importancia de la misma radica en que la organización debería verificar, y en su caso valorar de cara a la adjudicación, si los concurrentes cumplen los requisitos de seguridad y privacidad requeridos, desde la misma homologación, y, en su caso, valorar el grado de cumplimiento.

Se verificará para cada participante si cumple con las condiciones que se han establecido en el pliego.

3.3. Contratación

Sin entrar en consideraciones jurídicas, el hecho es que existe la posibilidad de que en el

contrato se recojan aspectos diferentes e, incluso no concordantes, con lo que se estableció en el pliego, con tal de que sean aceptadas por las partes contratantes.

Considerando esa capacidad de negociar de las partes, desde la óptica de la gestión de riesgos, en concreto del de privacidad, es necesario prestar atención al contrato con el fin de verificar si se recogen las salvaguardas exigidas o si, en su caso, se produce alguna alteración de las condiciones previstas que lleven a un incremento del riesgo de privacidad o sus consecuencias.

4. Desarrollo del contrato

Durante el desarrollo del contrato o del acuerdo de colaboración, deberá verificarse con la periodicidad necesaria que, efectivamente, se cumplen con todas las condiciones que han ido imponiéndose desde el inicio de la relación con el tercero y desde el momento en que se concibió el servicio.

Disponer de un procedimiento implantado para la valoración periódica del servicio prestado, en la que se incluyan aspectos de seguridad y privacidad (además de los meramente técnicos), es un sistema recomendable.

5. Fase postcontractual

Una vez finalizada la relación contractual deben seguir operando todos aquellos aspectos destinados a preservar los activos de la entidad, incluso los intangibles como reputación y, en particular, mantener la confidencialidad sobre la información y datos a los que ha accedido con motivo de esta relación contractual.

En este mismo orden, deberán preverse los mecanismos necesarios para que el tercero proceda a la devolución de la documentación en su poder, o en su caso a su destrucción verificada. Manteniendo y haciendo extensiva a sus empleados, el deber de confidencialidad.

Materialización: apuntes para posibles metodologías de evaluación del riesgo de privacidad

Como instrumentos para llevar a cabo lo expresado anteriormente, se deberá contar con metodologías de análisis y evaluación eficaces y realistas; con la particularidad de que deberán abarcar todas las fases mencionadas.

Mediante esta verificación se determinará si el candidato a proveedor cumple los requisitos mínimos de seguridad, o en caso contrario, si debe ser descartado como tal o aceptado con la condición de que adopte determinadas salvaguardas. Es recomendable que dicho test se acompañe de documentación acreditativa.

En la fase de licitación, la organización debe evaluar los riesgos del servicio que pretende y, en consecuencia, establecer las necesidades de seguridad en el pliego.

De los participantes en la licitación, se verificará el cumplimiento de las condiciones impuestas en el pliego. En esta fase es recomendable exigir certificaciones de seguridad que avalen su gestión.

El adjudicatario o el tercero que ya esté desarrollando el servicio o colaborando con nuestra organización debería someterse a auditorías suficientes para evaluar de forma fehaciente su nivel de seguridad. Para posibilitarlas es necesario prever su realización en los mismos pliegos y/o en el contrato.

La consecuencia de estas evaluaciones derivará en la adopción de medidas correctoras, formalizadas a través de un plan de acción.

Para finalizar es necesario mencionar que la eficacia en la aplicación de este proceso exige el concurso de múltiples áreas de la empresa: compras, jurídica, seguridad, etc. así como el compromiso de la dirección.

Más información en:
www.ismsforum.es

 @ISMSForum

 ISMS Forum

isms forum dpi