El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD)

Este documento, elaborado por la Autoridad Catalana de Protección de Datos en colaboración con la Agencia Española de Protección de Datos y la Agencia Vasca de Protección de Datos, tiene como objetivo identificar los puntos clave a tener presentes en el momento de establecer la relación entre el responsable del tratamiento y el encargado del tratamiento, así como identificar las cuestiones que afectan de forma directa a la gestión de la relación entre ambos.

Asimismo pretende ofrecer orientaciones, a modo de recomendación, para confeccionar el documento que regule dicha relación.

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

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales. Así, podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales (por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores) y otros que tratan datos personales sólo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento (por ejemplo el gestor de un servicio público municipal).

Pese a que la definición puede parecer clara, en la práctica se dan multitud de situaciones donde puede ser difícil deslindar cuándo estamos frente a un encargado o a un responsable del tratamiento. Para facilitar esta distinción, debemos tener en cuenta que corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones de quien le encomienda un determinado servicio, respecto al correcto tratamiento de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio.

Cuando sea de aplicación el texto Refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, debe tenerse en cuenta que dicha ley prevé (disposición adicional 26ª) que, cuando la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, el contratista tendrá la

consideración de encargado del tratamiento. En estos casos también será de aplicación el régimen establecido en el RGPD.

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

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte.

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

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por el responsable del tratamiento.

4.- ¿Puede el responsable del tratamiento elegir cualquier encargado del tratamiento?

El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del encargado.

El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.

Para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o la posesión de un certificado de protección de datos pueden servir como mecanismos de prueba.

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

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento.

En cualquier caso, ya se trate de un acuerdo o de otro acto jurídico, su contenido debe reunir los requisitos establecidos en el RGPD, a los que más adelante se hace referencia.

El contenido del acto o acuerdo puede basarse en cláusulas tipo establecidas por la Comisión Europea o por la autoridad de control, inclusive cuando formen parte de una certificación otorgada al responsable o al encargado del tratamiento.

Los modelos de cláusulas que se incluyen en el Anexo 1 de este documento no tienen la consideración de cláusulas tipo a los efectos del artículo 28.8 del RGPD, sino que son simplemente un modelo orientativo para que los diferentes responsables puedan adaptarlo a las necesidades derivadas de su propia organización.

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

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

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

No, el Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

Por otra parte, el RGPD también se aplicará al tratamiento de datos personales de interesados que residan en la Unión realizado por un encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

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

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

8.- ¿Existe un régimen especial para la contratación de un encargado que no esté establecido en el territorio de la Unión Europea o que efectúe el tratamiento fuera del territorio de la Unión?

La comunicación de datos personales, en el marco de un acuerdo de encargado del tratamiento, a un país que no forme parte de la Unión se rige por la regulación establecida en el Reglamento para las transferencias internacionales.

La transferencia a un tercer país en ningún caso puede suponer una reducción del nivel de protección de las personas que establece el Reglamento. Este principio también se aplica en las transferencias posteriores de datos personales, desde el tercer país a otro tercer país o una organización internacional.

Para la transferencia de datos a países que no garantizan un nivel de protección adecuado, el responsable deberá acreditar que el encargado del tratamiento está en disposición de ofrecer garantías adecuadas y, en todo caso, garantizar que los interesados cuenten con derechos exigibles y acciones legales efectivas.

9.- ¿Si se externaliza las funciones del delegado de protección de datos a un tercero, éste tiene la consideración de encargado del tratamiento?

Sí, el RGPD prevé que el delegado de protección de datos debe poder acceder a los datos que se traten. Por tanto, deberá formalizarse un encargo del tratamiento.

10.- ¿Es necesario informar a los interesados de la contratación de un encargado del tratamiento?

El RGPD no establece la obligación de informar respecto a la contratación de un encargado del tratamiento. Pese a esto, en determinadas circunstancias (atendiendo, por ejemplo, a la naturaleza del tratamiento o de los datos tratados, o por otras circunstancias concurrentes) puede ser aconsejable dar esta información para una mayor transparencia en el tratamiento de los datos personales.

11.- ¿Cuál es el contenido mínimo de un acuerdo de encargo del tratamiento?

Como mínimo debe establecerse el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

En particular, el acuerdo o acto debe contener:

A.- Las instrucciones del responsable del tratamiento

Se debe documentar de forma precisa las instrucciones respecto del encargo realizado. Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo. Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado.

La sujeción a las instrucciones del responsable deberá producirse igualmente en el caso de las transferencias internacionales de datos que puedan producirse como consecuencia de la prestación del servicio. Si el encargado del tratamiento está obligado legalmente, por el Derecho de la Unión o de un Estado miembro, a transferir datos a un tercer país deberá informar al responsable antes de llevar a cabo el tratamiento, salvo que tal derecho lo prohíba por razones importantes de interés público.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado deberá informar inmediatamente al responsable.

B.- El deber de confidencialidad

Hay que establecer la forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria.

El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable del tratamiento.

C.- Las medidas de seguridad

El acuerdo debe establecer la obligación del encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con lo establecido en el artículo 32 del RGPD.

Corresponde al responsable del tratamiento realizar la evaluación de riesgos para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de las personas afectadas. Así mismo el encargado también debe evaluar los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías, recursos etc.) y otras circunstancias que puedan incidir en la seguridad, como por ejemplo que el encargado lleve a cabo otros tratamientos.

A partir de aquí, la determinación de las medidas de seguridad concretas puede realizarse a través de una lista exhaustiva de las mismas o de la remisión a un estándar o marco nacional o internacional reconocido.

Así, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y las libertades de las personas físicas, el responsable y el encargado del tratamiento establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente que, en su caso, incluyan, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La adhesión a códigos de conducta o la posesión de una certificación son elementos que sirven para demostrar el cumplimiento de los requisitos anteriormente indicados.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

D.- El régimen de la subcontratación

El acuerdo debe establecer el régimen de subcontratación. El RGPD exige la autorización previa por escrito del responsable del tratamiento para que el encargado

del tratamiento pueda recurrir a otro encargado (subencargado) para desarrollar el servicio encomendado, cuando esto conlleve el tratamiento de los datos personales por parte de un tercero.

Esta autorización puede ser específica (identificación de la entidad concreta) o general (sólo autorizando la subcontratación, pero sin concretar la entidad).

En el supuesto que la autorización sea de carácter general, el encargado informará al responsable de la incorporación de un subencargado o su sustitución por otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

Puede ser de utilidad establecer en el acuerdo o acto la forma (que en todo caso deberá constar por escrito) y el plazo para que el responsable pueda manifestar su oposición.

En todo caso, el subencargado del tratamiento debe estar sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y en la misma forma (acuerdo por escrito o acto jurídico vinculante) que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

Cuando sea aplicable la legislación de contratos del sector público, habrá que tener en cuenta también las disposiciones específicas previstas en dicha ley.

E.- Los derechos de los interesados

Hay que establecer la forma en la que el encargado del tratamiento asistirá al responsable en el cumplimento de la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD:

- Acceso a datos personales
- Rectificación
- Supresión (derecho al olvido)
- Limitación del tratamiento
- Portabilidad de datos
- Oposición
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

El acuerdo deberá establecer de forma clara si corresponde al encargado del tratamiento atender y dar respuesta a las solicitudes de estos derechos o bien

establecer expresamente que su única obligación es comunicar al responsable del tratamiento que se ha ejercido un derecho.

En el primer supuesto, el acuerdo debe establecer la forma y los plazos para atender o, en su caso, dar respuesta a las solicitudes de ejercicio de derechos. En el segundo supuesto, debe establecerse la forma y el plazo en que la solicitud y, en su caso, la información correspondiente al ejercicio del derecho se debe comunicar al responsable del tratamiento.

En cuanto al derecho de información de las personas afectadas, se trata de un derecho no sujeto a solicitud y, por tanto, no sujeto a las previsiones del artículo 28.3.e) del RGPD. Pese a ello, en aquellos casos en que el encargado deba realizar la recogida de datos es recomendable establecer en el acuerdo o acto jurídico la forma y el momento en que debe darse el derecho de información.

F.- La colaboración en el cumplimiento de las obligaciones del responsable

Se debe establecer la forma en que el encargado ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las Autoridades de Protección de Datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas.

El cumplimiento de esta obligación queda supeditado a la naturaleza del tratamiento realizado y a la información que esté a disposición del encargado.

El responsable puede delegar en el encargado el cumplimiento de estas obligaciones.

G.- El destino de los datos al finalizar la prestación

Hay que prever si, una vez finalice la prestación de los servicios de tratamiento, el encargado del tratamiento debe proceder a la supresión o a la devolución de los datos personales y de cualquier copia existente, ya sea al responsable o a otro encargado designado por el responsable.

El acuerdo debe establecer de forma clara cuál de las dos opciones es la elegida por el responsable, así como la forma y el plazo en que debe cumplirse.

En todo caso, los datos deberán ser devueltos al responsable cuando se requiera la conservación de los datos personales, en virtud del Derecho de la Unión o de los Estados miembros.

No obstante, el encargado puede conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

H.- La colaboración con el responsable para demostrar el cumplimiento

Es preciso establecer la obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor autorizado por el responsable.