Contratos de encargado de tratamiento y medidas de seguridad en el marco del RGPD

A tenor de las últimas resoluciones de la Agencia Española de Protección de Datos (AEPD), **que han sancionado contratos de encargo de tratamiento por su carácter genérico e insuficiente**, consideramos conveniente recordar a nuestros clientes la importancia de contar con contratos de encargo debidamente adaptados al artículo 28 del RGPD.

Estos contratos deben definir de manera clara las finalidades, categorías de datos y medidas de seguridad aplicables, ya que la práctica reciente demuestra que la mera reproducción de disposiciones legales no resulta suficiente y expone al responsable del tratamiento a importantes riesgos sancionadores.

¿Qué es un contrato de encargado de tratamiento?

Cuando una empresa encarga a un tercero el tratamiento de datos personales, debe asegurarse de que ese proveedor ofrece garantías suficientes en materia de seguridad y cumplimiento normativo, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

¿Qué contenido mínimo debe cubrir un Contrato de Encargado del Tratamiento?

El artículo 28.3 del RGPD establece que el contrato debe recoger el **objeto, duración, naturaleza y finalidad del tratamiento**, así como los tipos de datos personales y categorías de interesados, y las obligaciones y derecho del responsable.

En particular, el contrato estipulará que el encargado:

- Tratará los datos únicamente siguiendo instrucciones documentadas del responsable.
- Garantizará la confidencialidad del personal autorizado.
- Adoptará medidas de seguridad adecuadas (art. 32 RGPD).
- Respetará las condiciones para subcontratar (arts. 28.2 y 28.4).
- Asistirá al responsable en el cumplimiento de sus obligaciones (ejercicio de derechos, brechas, evaluaciones de impacto).
- Suprimirá o devolverá los datos al finalizar el servicio.
- Pondrá a disposición del responsable la información necesaria para demostrar cumplimiento y facilitar auditorías.

Resoluciones sancionadoras recientes por insuficiente desarrollo del Contrato de Encargo de Tratamiento

Las Directrices 07/2020 del Comité Europeo de Protección de Datos (EDPB) ya advirtieron que los contratos de encargo de tratamiento deben adaptarse a cada relación concreta, recogiendo instrucciones claras y medidas de seguridad específicas y verificables.

En línea con este criterio, las últimas resoluciones de la AEPD muestran una clara tendencia: los contratos de encargo genéricos ya no son aceptables. La Agencia exige que el responsable pueda acreditar que el contrato detalla con precisión el objeto del tratamiento, las categorías de datos y las medidas de seguridad aplicables. Estos criterios se reflejan en dos expedientes recientes:

- En el expediente N.º: EXP202317228**,** las deficiencias contractuales llevaron a sancionar a la entidad por ***"limitarse a reproducir las disposiciones del RGDP"*** porque no detallaba el objeto del tratamiento con suficiente claridad ni las medidas técnicas y organizativas aplicables, impidiendo al responsable evaluar su adecuación al riesgo. el contrato de encargo incluía una cláusula bajo el título "Medidas de seguridad" que se limitaba a reproducir el artículo 32.1 RGPD. **No describía controles concretos** de gobernanza, accesos, cifrado o monitorización, ni preveía la obligación de someter cambios a la aprobación previa del responsable. Tampoco contemplaba revisiones periódicas. La Agencia consideró que esta falta de detalle impedía al responsable cumplir su **deber de responsabilidad proactiva**.

- La AEPD constató en el expediente N.º: EXP202318311 que ***"el contrato de encargo tiene que incorporar y estar adaptado a los plazos de conservación del tratamiento."***. El contrato debe incluir instrucciones claras al encargado y definición de las categorías de datos y de interesados afectados. aunque existían referencias a **medidas de seguridad**, estas eran **genéricas e insuficientes**. Algunas de ellas —como la implantación de controles técnicos— se adoptaron solo después de la brecha de seguridad, lo que evidenció que no había mecanismos efectivos de monitorización, continuidad ni gestión de riesgos.

Observación: la Agencia advierte que *"reproducir el artículo 32.1 del RGPD no satisface el nivel de detalle exigido por el artículo 28.3 del RGPD* ***al no definir con claridad qué medidas debe implementar el encargado lo que impide evaluar la adecuación al riesgo y la trazabilidad del cumplimiento normativo."***

¿Cómo deben concretarse las Medidas de Seguridad en un contrato de encargado de tratamiento?

- Definir con precisión el **alcance de los tratamientos**, sistemas y datos que estén cubiertos, especificando los controles exigibles en materia de accesos, cifrado, monitorización, continuidad y gestión de vulnerabilidades.
- Cualquier **modificación en las medidas de seguridad** o en la cadena de subencargados deberá contar con **autorización previa** y por escrito del responsable, asegurando la trazabilidad de la decisión adoptada.
- **Mecanismos** claros de detección, respuesta y notificación **de brechas de seguridad**, y garantizar la asistencia del encargado al responsable.
- Establecer **cómo se conservarán los datos** durante toda la relación contractual (retención, limitaciones de uso y control de accesos) y prever la supresión o devolución de los datos.

- Se debe fijar la **periodicidad de auditorías y revisiones**, así como los registros e informes que el encargado pondrá a disposición del responsable para acreditar el cumplimiento y facilitar las inspecciones necesarias.

¿Qué consecuencias tiene el incumplimiento de estas condiciones?

Tanto el EDPB en sus Directrices 07/2020 como la AEPD en sus resoluciones subrayan que un contrato de encargado de tratamiento genérico carece de validez práctica y expone al responsable a sanciones.

Dependiendo de la gravedad del caso concreto, se clasifican en:

- **Multas administrativas de 10.000.000 EUR** como máximo o, tratándose de una empresa, de una **cuantía equivalente al 2 % como máximo del volumen de negocio total anual** global del ejercicio financiero anterior, optándose por la de mayor cuantía
- **Multas administrativas de 20.000.000 EUR** como máximo o, tratándose de una empresa, de una **cuantía equivalente al 4 % como máximo del volumen de negocio total anual** global del ejercicio financiero anterior, optándose por la de mayor cuantía.