**ANEXO 18**

**MODELO ACUERDO ENCARGADO DEL TRATAMIENTO DE LOS DATOS PERSONAES**

**CS/AH01/1101446911/25/PSS**

El autor de este modelo es la Oficina del DPD de Salud.

**INTRODUCCIÓN**

Tal como se indica en el documento 8.1 relativo a la determinación del rol de los participantes en el tratamiento de los datos, podrá actuar como encargado del tratamiento cualquier persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El encargado del tratamiento deberá cumplir con las obligaciones siguientes:

* Tratar los datos atendiendo a las instrucciones proporcionadas por el responsable.
* Ayudar al responsable mediante la aplicación de las medidas técnicas y organizativas que se consideran necesarias.
* Asistir al responsable para garantizar el cumplimento en materia de seguridad del tratamiento, notificación de violaciones de seguridad o realización de evaluaciones de impacto.
* Podrá determinar elementos propios de su especialidad de tipo esencial del tratamiento.
* Podrá delegar algunas tareas, si así lo acepta el responsable.
* Colaborar con el responsable.

El acuerdo de encargo de tratamiento deberá cumplir con el contenido mínimo previsto en el art. 28 del RGPD, en concreto deberá hacer referencia a los aspectos siguientes:

* Objeto del contrato
* Duración
* Naturaleza y finalidad del tratamiento
* Tipología de datos personales tratados
* Categorías de interesados afectados
* Obligaciones y derechos del responsable

A continuación, se adjunta un modelo de encargo de tratamiento con indicación de los contenidos comentados en les líneas anteriores.

MODELO DE ACUERDO DE ENCARGO DE TRATAMIENTO

Acuerdo de encargo de tratamiento de datos de carácter personal entre \_\_\_\_\_\_\_ i \_\_\_\_\_\_\_ *[indicar les partes que suscriben el acuerdo]*

REUNIDOS

De un lado, ......................................... *[indicar nombre y apellidos del responsable]*, como responsable de los tratamientos de protección de datos de ....................................... *[indicar nombre de la entidad]*, entre los que se incluye el tratamiento relativo a .......................... *[indicar nombre del tratamiento]*................................................., en el ejercicio de las funciones que le confiere el Reglamento  (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las persones físicas en lo que hace referencia al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).

I del otro, el/la señor/a ....................... *[indicar nombre y apellidos]* ..........., *[especificar cargo]*........., en representación de ............ *[nombre de la entidad]* .........., de acuerdo con ..........*[justificar representación]*........., como encargado del tratamiento,

Ambas partes, en el ejercicio de las funciones que las que están legalmente asignadas, reconociéndose recíprocamente la capacidad legal necesaria para obligarse de común acuerdo,

**MANIFIESTAN**

1. Que........................... *[indicar nombre del responsable]*, de acuerdo con las competencias que tiene atribuidas, le corresponden la realización de ................................. *[especificar las competencias en las que se encuentra incluida el objeto del tratamiento]* ..........................................
2. Que la empresa contratista ................................... *[en su caso]* tiene por objeto ................................................ *[indicar finalidad/es]*.
3. *[Hacer referencia al contrato que hace necesario firmar el acuerdo y otra información que sea necesaria; incluir, en su caso, el núm. De expediente contrato. Ejemplo: Ambas partes han firmado un contracte per X, con expediente X]*
4. Dado que la ejecución del contrato mencionado por parte de ... *[indicar empresa contratista*] comporta tratar datos personales de las cuales es responsable ... *[indicar órgano de contratación*], ...... *[*indicar *nombre de la empresa contratista]* tiene la consideración de encargada del tratamiento, de acuerdo con el RGPD i LOPDGDD.
5. Que ........ *[nombre empresa contratista]* dispone de la capacidad y los recursos necesarios para garantizar que, en su calidad de encargado de tratamiento, aplica las medidas técnicas y organizativas apropiadas para cumplir con lo que establece la legislación de protección de datos mencionada.
6. La necesidad de firmar un acuerdo de encargado de tratamiento de datos de carácter personal en relación con el contrato mencionado, en los términos que establecen los artículos 28 del RGPD y 33 de la LOPDGDD.

**CLÀUSULAS**

**Primero. - Objeto del acuerdo de encargo**

Mediante este acuerdo de encargo se habilita........................... *[indicar nombre de la entidad encargada]*, en calidad de encargado de tratamiento (en adelante, el encargado), para tratar por cuenta de ................ *[indicar nombre de la entidad responsable*] (en adelante, el responsable) los datos de carácter personal necesarios para la realización de ........................................ *[indicar el objeto del encargo de tratamiento].*

El tratamiento consistirá en ........................................[*descripción detallada del tratamiento y de les actuaciones concretas a realizar*].

**Segunda. - Identificación de la información afectada**

Para ejecutar las prestaciones derivadas del cumplimiento del objeto de este acuerdo de encargo, el responsable pone a disposición del encargado la información siguiente: *[indicar una opción]*

*OPCIÓN A*

*[Especificar tipo/categorías de datos: identificativos, de características personales, datos de salud: clínicas, etc.].*

*[Especificar categorías de personas interesadas: colectivos vulnerables, pacientes, profesionales sanitarios, ciudadanos, etc.].*

..... que se describe a continuación:

*OPCIÓN B*

*[En el caso que el objeto del contrato comporte el tratamiento de muchas categorías de datos personales y/o de personas interesadas, es mejor remitirse a un anexo en el que consten. Se propone redactado siguiente:]*

...... corresponden a los tratamientos que es relacionen a l’annex 1.

**Tercero. - Duración**

La vigencia de este acuerdo de encargo queda vinculada a la duración del contrato suscrito que se ha identificado en será de ..................... *[indicar vigencia y fundamentarla] ....................*.

**Cuarto. - Obligaciones del encargado de tratamiento**

El encargado de tratamiento y todo su personal se obligan a:

1. Usar los datos personales objeto de tratamiento, o los que recoja para su inclusión, solo para la finalidad objeto de este acuerdo de encargo. En ningún caso pueden usar los datos para finalidades propias.
2. Tratar los datos únicamente de acuerdo con las instrucciones documentadas del responsable de tratamiento.

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

1. Limitar el acceso a los datos personales tratados a los miembros de su personal en la medida que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del encargo. El encargado ha de garantizar que las personas autorizadas para tratar los datos personales se han comprometido a respetar la confidencialidad o están sujetos a una obligación de confidencialidad de naturaleza estatutaria, así como a cumplir las medidas de seguridad correspondientes, de las cuales deberá informarse convenientemente.

Mantener a disposición del responsable la documentación que acredita su cumplimiento.

1. Mantener el deber de secreto respecto a les datos personales a los que haya tenido acceso en virtud de este acuerdo de encargo, hasta después que finalice el objeto.
2. No comunicar los datos a terceras personas, salvo que tenga la autorización expresa del responsable de tratamiento en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados de tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable ha de identificar, previamente y por escrito, la entidad a la que se han de comunicar los datos, la finalidad, los dato a comunicar y las medidas de seguridad que debe aplicarse para proceder a la comunicación.

1. Las transferencias de datos a un tercer país o a una organización internacional por parte del encargo, únicamente se pueden realizar siguiendo instrucciones documentadas del responsable o en virtud de una exigencia expresa del derecho de la Unión o de un estado miembro al que esté sujeto el encargo.
2. Subcontratación

*[Escoger una de les opciones]*

*OPCIÓN A:*

No se pueden subcontratar ninguno de los tratamientos de datos incluidos en las prestaciones que forman parte del objeto de este encargo.

*OPCIÓN B:*

Se pueden subcontratar algunos de los tratamientos de datos previstos en el objeto de este encargo.

Si hace falta subcontratar algún tratamiento, este hecho se ha de comunicar previamente y por escrito al responsable, con una antelación de ........................... *[indicar el plazo]*. Hace falta indicar los tratamientos que es pretenden subcontratar e identificar de forma clara e inequívoca la empresa subcontratista y sus datos de contrato. La subcontratación se llevará a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tiene la condición de encargado de tratamiento, está obligado igualmente a cumplir las obligaciones que este documento establece para el encargado de tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de manera que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, mesures de seguridad…) y con los mismos requisitos formales que él, por lo que hace al tratamiento adecuado de los datos personales y a la garantía de los derechos de las personas afectadas. Si el subencargado lo incumple, el encargado inicial continua siendo plenamente responsable delante del responsable por lo que hace al cumplimiento de las obligaciones.

En todo caso, el responsable ha de estar informado de tota la cadena de subcontratación.

1. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
2. Asistir al responsable de tratamiento en la respuesta al ejercicio de los derechos siguientes:
3. Acceso, rectificación, supresión y oposición.
4. Limitación del tratamiento.
5. Portabilidad de datos.
6. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y a no ser objeto de decisiones individualizadas automatizadas ante el encargado del tratamiento, este deberá comunicarlo por correo electrónico a la dirección indicada en la cláusula octava de este contrato de encargo. La comunicación deberá realizarse de forma inmediata y, en ningún caso, más allá del día siguiente al de la recepción de la solicitud, teniendo en cuenta que, si se ha recibido en un día no laborable, se entenderá recibida el primer día laborable siguiente, junto, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

El encargado no debe dar respuesta por sí mismo a dichas solicitudes salvo que haya sido autorizado por el responsable.

1. Derecho de información.

*[Escoger una de las opciones]*

*OPCIÓN A*

El encargado del tratamiento debe facilitar, en el momento de recoger los datos, la información relativa a los tratamientos de datos que se llevarán a cabo. La redacción y el formato en que se facilitará la información deberán consensuarse con el responsable, antes de iniciar la recogida de los datos.

*OPCIÓN B*

Corresponde al responsable facilitar el derecho de información en el momento de recoger los datos.

1. El encargado también debe asistir al responsable para garantizar el cumplimiento de las siguientes obligaciones, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga:
2. La obligación de realizar una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales, cuando sea probable que un determinado tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas.
3. La obligación de consultar a la autoridad de control antes de comenzar el tratamiento, cuando la evaluación de impacto relativa a la protección de datos evidencie que el tratamiento comporta un alto riesgo si el responsable no adopta las medidas necesarias para mitigarlo.
4. La obligación de garantizar que los datos personales sean exactos y estén actualizados.
5. Poner a disposición del responsable toda la información necesaria para demostrar que cumple con sus obligaciones, así como para realizar las auditorías o inspecciones que lleve a cabo el responsable o cualquier otro auditor autorizado por él.
6. Notificación de violaciones de la seguridad de los datos.

En el supuesto de violación de la seguridad de los datos personales, el encargado ha de colaborar con el responsable y ayudarlo a dar cumplimiento a las obligaciones que le atribuye el RGPD, de la manera siguiente:

1. Cuando se trate de una violación de la seguridad de datos personales tratados por el responsable, el encargado ha de asistir al responsable en las siguientes acciones:
2. Notificar la violación de seguridad de los datos personales a la autoridad de control sin dilación indebida desde tener constancia, en su caso.
3. Preparar toda la información relevante para documentar y comunicar la incidencia, y que ha de incluir como mínimo:

* Descripción de la naturaleza de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados y las categorías y el número aproximado de registres de datos personales afectadas.
* Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
* Descripción de las medidas adoptadas o propuestas para remediar la violación de la seguridad de los datos personales, incluidas, en su caso, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en qué no lo sea, la información se ha de facilitar de manera gradual sin dilación indebida.

1. Comunicar la violación de seguridad de los datos personales al interesado sin dilación indebida desde qué tenga constancia, en su caso.
2. Cuando se trate de una violación de la seguridad de datos personales tratados por el encargado:

Ha de informar el responsable del tratamiento, sin dilación indebida y en cualquier caso antes de 24 horas desde tener constancia, de las violaciones de la seguridad de los datos personales a su cargo de las cuales tenga conocimiento, juntamente con toda la información relevante para documentar y comunicar la incidencia, por correo electrónico al correo indicado en la cláusula octava de este acuerdo de encargo.

Si se dispone, debe facilitar, como mínimo, la información especificada en el apartado b) del punto 1 y, adicionalmente, el nombre y los datos de un punto de contacto en el que poder obtener más información.

Si no es posible facilitar la información simultáneamente, y en la medida en qué no lo sea, la información se ha de facilitar de manera gradual sin dilación indebida.

1. Implementar les medidas de seguridad oportunas de acuerdo con el nivel de riesgo determinado para cada tratamiento objeto del encargo que se derivan de la aplicación del Esquema Nacional de Seguridad (ENS) *[seria recomendable especificar las medidas de seguridad que se aplican descritas de manera concreta en un anexo a este acuerdo].*

En todo cas, debe implantar mecanismos para:

1. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2. Restaurar la disponibilidad y el acceso a los datos personal de forma rápida, en caso de incidente físico o técnico.
3. Verificar, evaluar i valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4. Anonimizar y cifrar los datos personales, en su caso.

También ha de adoptar todo tipo de medidas que, teniendo en cuenta el conjunto de tratamientos que realiza, sean necesarias para garantizar un nivel de seguridad adecuado al riesgo.

La documentación relacionada con la gestión de los riesgos, incluyendo el resultado de las auditorias periódicas que se realicen, puede ser solicitada en cualquier momento por el responsable de tratamiento.

1. Designar un delegado de protección de datos, si el encargo se encuentra incluido en uno de los supuestos previstos en el artículo 37.1 del Reglamento, y comunicar la identidad y los datos de contacte al responsable.
2. Destinación de los datos

Retornar al responsable del tratamiento los datos de carácter personal y, en su caso, los soportes donde consten, una vez completa la prestación.

La devolución ha de comportar el borrado total de los datos existentes en los equipos informáticos usados por el encargado y la supresión de todas las copias existentes.

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

1. En el cas de uso de servidores, comunicar el lugar donde estarán ubicados y des de donde se prestarán los servicios asociados a éstos, así como cualquier cambio que se produzca en relación con esta información.
2. Incorporar los tratamientos que lleva a cabo en ejecución de este contrato en su registro de actividades del tratamiento efectuadas por cuenta de un responsable, con el contenido del artículo 30.2 del RGPD.

*[Esta obligación no es exigible a las empresas u organizaciones que ocupen menos de 250 persones salvo que concurra alguna de las circunstancies siguientes:*

1. *Si es probable que haya un riesgo para derechos y libertades de los sujetos.*
2. *Si el tratamiento no es ocasional*
3. *Si incluye categorías especiales de datos (art.9 RGPD) o infracciones y condenas penales.*

*En estos casos el encargado sí ha de incluir su RAT a estos tratamientos].*

**Quinta. - Obligaciones del responsable de tratamiento**

Corresponde al responsable de tratamiento:

1. Entregar al encargado los datos a les cuales se refiere la cláusula segunda de este acuerdo de encargo.
2. Hacer una evaluación del impacto sobre la protección de datos personales de las operaciones de tratamiento que ha de efectuar el encargado, si fuese preceptivo.
3. Hacer las consultas previas que correspondan.
4. Velar, antes y durante todo el tratamiento, para que el encargado cumpla la normativa en materia de protección de datos.
5. Supervisar el tratamiento, incluida la ejecución de inspecciones y auditorias.

**Sexta. - Derechos del responsable de tratamiento:**

El responsable del tratamiento tiene derecho a:

1. Obtener del encargado toda la información que considere necesaria relativa a los datos y los tratamientos que se describen en la cláusula segunda, para que pueda cumplir con sus obligaciones como responsable.
2. Obtener la asistencia del encargado para atender las peticiones e inspecciones de cualquier autoridad de control cuando los tratamientos objeto de aquellas sean las que realiza el encargado.
3. Ser compensado por el encargo por los daños y perjuicios que soporte como consecuencia del incumplimiento de las obligaciones del encargado o de sus subcontratistas.

**Séptima. - Modificación del acuerdo de encargo**

Este acuerdo de encargo de tratamiento de datos personales se podrá modificar de manera expresa y de común acuerdo entre las partes, mediante la firma de la adenda correspondiente.

**Octava. - Comunicaciones y notificaciones**

1. Las comunicaciones dirigidas al responsable del tratamiento se enviarán a:

*[determinar por el responsable, dirección postal y correo electrónico]*

1. Las comunicaciones dirigidas al encargo de tratamiento se enviarán a:

*[determinar por el encargado dirección postal y correo electrónico]*

1. Las comunicaciones en los casos de vulneraciones de seguridad se dirigirán, con copia al responsable funcional de que se trate, a la dirección electrónica siguiente:

*[determinar por el responsable dirección electrónica]*

En prueba de conformidad, ambas partes firman este acuerdo de encargo.

|  |  |
| --- | --- |
| ***[nombre y apellidos]*** | ***[nombre y apellidos]*** |
| Representante del responsable | Representante del encargo |
|  |  |