##

##  versión 03.12.2019

**ANEXO I**

**Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas**

*(Estas cláusulas tienen sólo carácter orientativo y deben adaptarse a las circunstancias concretas del tratamiento que se lleve a cabo)*

**1. Objeto y finalidad del encargo del tratamiento**

Mediante las presentes cláusulas se habilita a la entidad ..................................................., encargada del tratamiento, para tratar por cuenta de ..............................................................., responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de………………… . .

**El tratamiento consistirá en:** *(descripción detallada del servicio)*

Concreción de los tratamientos a realizar:

 Recogida  Registro

 Estructuración  Modificación

 Conservación  Extracción

 Consulta  Comunicación por transmisión

 Difusión  Interconexión

 Cotejo  Limitación

 Supresión  Destrucción

 Comunicación  Otros ……

**2. Identificación de la información afectada**

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad/órgano....................................., responsable del tratamiento, pone a disposición de la entidad ......................................, encargada del tratamiento, la información que se describe a continuación:

**• ...........**

**• ...........**

**• ...........**

Categorías de personas interesadas:*ciudadanos / usuarios / clientes / trabajadores / pacientes / menores / persones discapacitadas / ... (indicar la opción que proceda).*

**3. Duración**

El presente acuerdo tiene una duración de.......................[[1]](#footnote-1)

**4. Obligaciones del encargado del tratamiento**

El encargado del tratamiento y todo su personalse obliga a:

1. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
2. Tratar los datos de acuerdo con las instrucciones documentadas del responsable del tratamiento.

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 informará inmediatamente al responsable.

1. Incorporar los tratamientos que lleva a cabo en ejecución de este contrato a su registro de actividades del tratamiento efectuadas por cuenta de un responsable, con el contenido del artículo 30.2 del RGPD[[2]](#footnote-2).
2. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

1. Subcontratación

*(Escoger una de las opciones)*

***OPCIÓN A***

*No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporte el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.*

*Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de ...........................[[3]](#footnote-3), indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.*

*El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las*

*instrucciones que dicte el responsable. Corresponde al encargado inicial*

*regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que* *él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.*

***OPCIÓN B***

*Se autoriza al encargado a subcontratar con la empresa …..................................................... las prestaciones que comporten los tratamientos siguientes:*

*............................................................................*

*Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de ………………[[4]](#footnote-4).*

*El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.*

1. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.
2. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a seguir las instrucciones del responsable, a respetar la confidencialidad[[5]](#footnote-5) y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
3. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
4. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
5. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:
6. Acceso, rectificación, supresión y oposición
7. Limitación del tratamiento
8. Portabilidad de datos
9. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

 *(Escoger una de las opciones)*

***OPCIÓN A***

*El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.[[6]](#footnote-6)*

***OPCIÓN B***

*Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección ………… (dirección que indique el responsable). La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud[[7]](#footnote-7), juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.*

1. Derecho de información.

*(Escoger una de las opciones)*

***OPCIÓN A***

*El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.*

***OPCIÓN B***

*Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.*

1. Notificación de violaciones de la seguridad de los datos.

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de……..[[8]](#footnote-8), y a través de………, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
4. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

*(Escoger alguna o las dos opciones)[[9]](#footnote-9)*

***OPCIÓN A***

*Corresponde al encargado del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.*

*La comunicación contendrá, como mínimo, la información siguiente:*

1. *Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.*
2. *Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.*
3. *Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.*
4. *Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

*Si no es posible facilitar la información simultáneamente, se facilitará de manera gradual sin dilación indebida.*

***OPCIÓN B***

*Corresponde al encargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.*

*La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:*

1. *Explicar la naturaleza de la violación de datos.*
2. *Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.*
3. *Describir las posibles consecuencias de la violación de la seguridad de los datos personales.*
4. *Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*
5. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
6. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.
7. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
8. Implantar las medidas de seguridad siguientes:

*(Escoger una o las dos opciones)*

***OPCIÓN A***

Las medidas de seguridad siguientes, de acuerdo con la evaluación de riesgos realizada por[[10]](#footnote-10)……, en fecha ……:

***• ...........***

***• ...........***

***• ...........***

***OPCIÓN B***

Las medidas de seguridad que se deriven de la aplicación de[[11]](#footnote-11) ………

En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

También debe adoptar todas aquellas otras medidas que, teniendo en cuenta el conjunto de tratamientos que lleva a cabo, 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 auditorías periódicas que se realicen, puede ser solicitada en cualquier momento por el responsable del tratamiento.

1. Designar un delegado de protección de datos[[12]](#footnote-12) y comunicar su identidad y datos de contacto al responsable.
2. Destino de los datos.

 *(Escoger una de las tres opciones)*

***OPCIÓN A***

*Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.*

*La devolución debe comportar la destrucción de las copias y el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.*

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

***OPCIÓN B***

*Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.*

*La devolución debe comportar la destrucción de las copias y el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.*

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

***OPCIÓN C***

*Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.*

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

s) El contratista debe someterse a la normativa nacional y de la Unión Europea en materia de protección de datos. Esta obligación tiene la condición de obligación contractual esencial.[[13]](#footnote-13)

t) Cuando la ejecución del contrato implique la utilización de servidores por parte del contratista, la empresa adjudicataria deberá presentar, antes de formalizar el contrato, y cuando se produzca cualquier cambio durante la ejecución del contrato, una declaración sobre el lugar donde estarán ubicados los servidores y desde donde se prestarán los servicios asociados a estos.13

u) Los licitadores deberán indicar en su oferta si tienen previsto subcontratar los servidores o servicios asociados a estos y, en caso afirmativo, el nombre o el perfil empresarial de los subcontratistas, definido por referencia a las condiciones de solvencia profesional o técnica.13

**5. Obligaciones del responsable del tratamiento**

Corresponde al responsable del tratamiento:

1. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, antes y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
1. En algunos casos, en particular determinados casos sometidos al derecho administrativo (convenios, contratos de gestión de servicios públicos, etc.), la duración del encargo puede estar limitada por la duración establecida por la legislación vigente para la prestación de servicios. [↑](#footnote-ref-1)
2. La obligación indicada en el artículo 30.2 del RGPD no se aplicará a empresas ni organizaciones que ocupen menos de 250 personas salvo que concurra alguna de las siguientes circunstancias:

a) Si es probable que exista un riesgo para derechos y libertades de los sujetos.

b) Si el tratamiento no es ocasional.

c) Si incluye categorías especiales de datos (art 9 RGPD) o infracciones y condenas penales.

Si concurre alguna de estas circunstancias el encargado deberá incluir en el registro los tratamientos en los que concurran. [↑](#footnote-ref-2)
3. Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación. [↑](#footnote-ref-3)
4. Se recomienda establecer un plazo para que pueda oponerse. [↑](#footnote-ref-4)
5. Si existe una obligación de confidencialidad de naturaleza estatutaria deberá quedar constància expresa de la naturaleza y extensión de esta obligación. [↑](#footnote-ref-5)
6. A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado. [↑](#footnote-ref-6)
7. Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido. [↑](#footnote-ref-7)
8. El plazo debe ser inferior a 72 horas en cualquier caso. [↑](#footnote-ref-8)
9. Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado. [↑](#footnote-ref-9)
10. Indicar si la evaluación de riesgos ha sido realizada por el responsable o por el encargado del tratamiento. [↑](#footnote-ref-10)
11. Indicar el código de conducta, el sello, la certificación u otro estándar donde están definidas las medidas aplicables, como sería el caso del Esquema Nacional de Seguridad (ENS) para las entidades definidas en el artículo 77.1 LOPDGDD y las empresas o fundaciones vinculadas a estas entidades (D.A. 1a LOPDGDD). [↑](#footnote-ref-11)
12. El delegado de protección de datos debe designarse cuando:

a) El tratamiento lo lleve a cabo una autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, por razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.

c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. [↑](#footnote-ref-12)
13. Las cláusulas de las letras s), t) y u) son obligatorias para los encargos del tratamiento establecidos en el marco de la legislación de contratos del sector público. Estas cláusulas deben constar en el Pliego de cláusulas administrativas particulares (art. 122.2 LCSP). [↑](#footnote-ref-13)