

TALLERES FORMATIVOS GRATUITOS PARA
ENTIDADES SIN ÁNIMO DE LUCRO

modo
dataprotección

Las herramientas clave para las
organizaciones del tercer sector en
materia de Protección de Datos

TALLER 4. CÓMO IDENTIFICAR LOS ENCARGADOS DEL TRATAMIENTO Y PREPARAR UN CONTRATO

Profesior: Antonio Borjas

DESCRIPCIÓN BREVE

El Taller 4 tiene como objetivo aprender a realizar un contrato de encargado de tratamiento. Las personas asistentes dispondrán del modelo de contrato de encargado de tratamiento propuesto por la Agencia Española de Protección de Datos para supuestos en que el encargado del tratamiento trate los datos en sus locales.

UNA INICIATIVA DE:



Coordinadora de
ONG para el **D**esarrollo
Región de Murcia

www.coordinadoraongdrm.org



Fundación
Pro Bono
España

www.probonoespana.org

FORMACIÓN IMPARTIDA POR:

C L I F F O R D
C H A N C E

Pérez-Llorca



Pinsent Masons



Ramón y Cajal
ABOGADOS

CON EL APOYO DE:



El presente documento no constituye ningún asesoramiento jurídico por parte de las y los profesionales del Derecho que lo distribuyen, sino que está elaborado con el único propósito de difundir conocimientos de interés general en torno a la normativa de protección de datos para que las entidades puedan basarse en el mismo para trabajar su documentación propia. Por tanto, los participantes de su elaboración están exonerados de cualquier responsabilidad por la utilización del mismo.

TALLER 4: REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

1.- Conceptos básicos

El **responsable del tratamiento** es el “propietario” de los datos. Decide sobre la finalidad y medios del tratamiento. Actúa con autonomía e independencia.

El **encargado del tratamiento** es una entidad que accede a los datos para prestar un servicio al responsable. No es “propietario” de los datos y actúa siempre siguiendo las instrucciones del responsable.

RESPONSABLE	ENCARGADO
Decide sobre la finalidad y medios del tratamiento de forma autónoma e independiente.	Obedece las órdenes del responsable, aunque puede tomar decisiones operativas con cierta autonomía.
Tiene una relación directa (por ejemplo, un contrato) con los afectados y actúa frente a estos en nombre propio.	Cuando interactúa con los afectados, lo hace en nombre del responsable, no en nombre propio.
Es el “propietario” de los datos.	Es un prestador de servicios.
Tiene obligaciones directas de conservación de los datos o cumple una obligación legal al tratar los datos.	Sigue las instrucciones del responsable.
Atiende el ejercicio de derechos.	Solo atenderá el ejercicio de derechos si se lo indica el responsable.
Notifica brechas de seguridad a la AEPD.	Informa de las brechas de seguridad al responsable y colabora en su investigación.

RESPONSABLE	ENCARGADO
Decide las bases de legitimación del tratamiento y redacta la política de privacidad o cláusula informativa.	No siempre aparece mencionado en la política de privacidad o cláusula informativa. Utiliza los textos redactados por el responsable.
TIENE PERSONALIDAD JURÍDICA PROPIA	TIENE PERSONALIDAD JURÍDICA PROPIA

2.- Marco legal básico

- ❑ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (“**RGPD**”). [Enlace a la norma.](#)
- ❑ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (“**LOPDGDD**”). [Enlace a la norma.](#)

Puedes encontrar información de utilidad en la página web de la Agencia Española de Protección de datos, y en particular, en la sección “Cumple tus obligaciones”. [Enlace a la sección.](#)

Y ADEMÁS...

Descarga de forma gratuita las Directrices de la Agencia Española de Protección de Datos para la elaboración de contratos entre responsables y encargados del tratamiento como complemento de este curso:

guia-directrices-contratos.pdf (aepd.es)

3.- Caso práctico propuesto y descripción del modelo facilitado

En la segunda sesión del taller 4 nos centraremos en la elaboración de un contrato de encargado de tratamiento.

Tened en cuenta que, conforme a la normativa de protección de datos, en caso de que un proveedor acceda a nuestros datos personales, deberemos suscribir el correspondiente contrato de encargado de tratamiento.

De acuerdo con lo anterior, en este taller os proponemos que escojáis entre vuestros proveedores uno que acceda a vuestros datos personales para poder prestar sus servicios. Por ejemplo, si vuestra entidad tiene externalizado la gestión de nóminas del personal, podréis escoger dicho proveedor.

Una vez que hayáis escogido a vuestro proveedor que acceda a datos personales, podéis utilizar el modelo de contrato de encargado de tratamiento que os proponemos a continuación.

El modelo de contrato de encargado del tratamiento es el propuesto por parte de la Agencia Española de Protección de Datos en sus [Directrices para la elaboración de contratos entre responsables y encargados del tratamiento.](#)

Tened en cuenta que el contrato de encargado de tratamiento debe contener los elementos establecidos en el artículo 28 del Reglamento General de Protección de Datos.

4.- Modelo propuesto

1. Objeto 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
- Estructuración
- Modificación
- Conservación
- Registro
- Extracción
- Consulta
- Comunicación por transmisión
- Difusión
- Interconexión
- Cotejo
- Limitación
- Supresión
- Destrucción

- Conservación
- Comunicación

2. Identificación de la información afectada

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

- [REDACTED]
- [REDACTED]

3. Duración

El presente acuerdo tiene una duración de [REDACTED]¹

Una vez finalice el presente contrato, el encargado del tratamiento debe **suprimir/devolver** al **responsable/devolver** a otro encargado que designe el responsable [**indicar la opción que proceda**] los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

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.

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, solo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones 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.

c. Llevar, por escrito, un registro² de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

² “Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.” (Art. 30.5 RGPD).

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
 - a) La seudoanonimización 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) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. 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.

e. Subcontratación

[Escoger una de las opciones]

Opción A *No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que*

comporten 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 de³, 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

³ Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

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 de⁴.

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas

⁴ Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

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.

- f) 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.

- g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad⁵ y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles

⁵ Si existe una obligación de confidencialidad de naturaleza estatutaria deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

convenientemente.

- h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

- i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

- j) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:
 - 1. Acceso, rectificación, supresión y oposición
 - 2. Limitación del tratamiento
 - 3. Portabilidad de datos
 - 4. 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 encargo⁶.

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 solicitud⁷, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k) Derecho de información

[Escoger una de las opciones]

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.

⁷ Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido.

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 información en el momento de la recogida de los datos.

I) 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 de⁸, 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.

⁸ El plazo debe ser inferior a 72 horas en cualquier caso.

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

- a) 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 interesado afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- b) 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.
- c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- d) 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

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.

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:

- a) 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.*
- b) Nombre y datos de contacto del delegado de protección de datos de otro punto de contacto en el que pueda obtenerse más información.*
- c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.*
- d) 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.

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:*

a) Explicar la naturaleza de la violación de datos.

b) 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.

c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

d) 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.

m) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n) Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner 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.

p) 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 por¹⁰, en fecha

-
-
-

Opción B Las medidas de seguridad establecidas en¹¹

.....

En todo caso, deberá implantar mecanismos para:

¹⁰ Indicar si la evaluación de riesgos ha sido realizada por el responsable o por el encargado del tratamiento.

¹¹ Indicar el código de conducta, el sello, la certificación u otro estándar donde están definidas las medidas aplicables.

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.

q) Designar un delegado de protección de datos¹² y comunicar su identidad y datos de contacto al responsable.

r) Destino de los datos

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, en 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.

[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 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 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.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
- b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
- c) Realizar las consultas previas que corresponda.
- d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

RECUERDA:

- ❑ Tendremos una segunda sesión **NO GRABADA** para revisar el trabajo que habéis realizado y resolver vuestras dudas. No obstante, puedes **enviar cualquier consulta o duda a nuestro equipo a través del correo mododataprotection@gmail.com**

- ❑ Si no contáis con proveedores que accedan a vuestros datos personales, podéis proponer cualquier supuesto que consideréis. Lo importante es que aprendáis a identificar los supuestos en los que un proveedor se considera encargado de tratamiento y que, en tal caso, sepáis que se debe suscribir el correspondiente contrato de encargado de tratamiento con un contenido mínimo.

- ❑ **La segunda sesión del taller será el día 7 de abril.**

