



## RECOMENDACIÓN

1 / 2 0 1 0

de la Agencia Catalana de Protección de Datos, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña

Abril 2010

## ÍNDICE

### **Capítulo 1.** *Disposiciones generales*

1. Objeto
2. Ámbito de aplicación
3. Concepto de responsable del fichero o del tratamiento
4. Concepto de encargado del tratamiento
5. Elección del modelo organizativo
6. El contrato o acuerdo de encargo del tratamiento
7. Contenido del contrato o acuerdo de encargo

### **Capítulo 2.** *El encargado del tratamiento en la contratación del sector público*

8. Carácter necesario de la figura del encargado del tratamiento
9. Pliegos de cláusulas administrativas y de prescripciones técnicas
10. Forma del contrato
11. Contratos menores
12. Subcontratación
13. Ejecución de contratos que no requiera el acceso a datos personales

### **Capítulo 3.** *El encargado del tratamiento en convenios, delegaciones interadministrativas, encargos de gestión y otras fórmulas análogas*

14. Supuestos de utilización de la figura del encargado del tratamiento
15. Acuerdo de encargo del tratamiento de datos
16. Transmisiones intradministrativas de datos
17. Subencargo del tratamiento

### **Capítulo 4.** *Efectos de la existencia de un encargo del tratamiento*

18. Régimen aplicable
19. Legitimación del tratamiento por parte del encargado
20. Deber de información
21. Vinculación a la finalidad
22. Instrucciones del responsable del fichero o tratamiento
23. Deber de confidencialidad
24. Régimen de comunicaciones
25. Encargos que impliquen transferencias internacionales de datos
26. Notificación al Registro de Protección de Datos de Cataluña
27. Ejercicio de derechos
28. Devolución o destrucción de los datos
29. Responsabilidad

### **Capítulo 5.** *Medidas de seguridad*

30. Medidas de seguridad aplicables
31. Auditoría
32. Tratamiento en los locales del responsable
33. Tratamiento en los locales del encargado
34. Documento de seguridad del responsable
35. Documento de seguridad del encargado
36. Responsable de seguridad
37. Delegación de autorizaciones
38. Prestación de servicios sin acceso a datos personales

### **Anexos**

## Recomendación 1/2010, de la Agencia Catalana de Protección de Datos, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña

Los datos de carácter personal necesarios para el funcionamiento de un servicio público o de una actividad pública son responsabilidad del ente titular del servicio o actividad de que se trate. Con el fin de compatibilizar esta circunstancia con la necesidad de externalización de determinados servicios o, en su caso, la colaboración interadministrativa en determinados ámbitos, deben adoptarse las medidas necesarias para garantizar en todo momento la autenticidad, la integridad y la confidencialidad de los datos tratados a fin de evitar la alteración, pérdida, tratamiento o acceso no autorizados.

Con este objetivo, la normativa de protección de datos prevé, con la denominación de encargado del tratamiento, una figura que permite el tratamiento de datos por cuenta del responsable de los datos. Se establecen así medidas adecuadas de seguridad, a la vez que se flexibiliza el régimen de comunicación de datos entre estas entidades.

El establecimiento de la figura del encargado del tratamiento ofrece la posibilidad que las entidades del sector público que externalicen servicios puedan conservar el control efectivo sobre el tratamiento, de manera que se garantice la continuidad del servicio, con independencia de que todas o algunas de las tareas materiales que implique el tratamiento las lleve a cabo otra persona o entidad. En estos supuestos, el ordenamiento mantiene para el fichero o tratamiento el régimen de creación, notificación y responsabilidad que correspondería al responsable del fichero, a la vez que flexibiliza el régimen de comunicación de datos previsto en la LOPD.

Procede, sin embargo, hacer una mención especial a las exigencias derivadas de la normativa de contratación pública. En el caso de Cataluña, la Recomendación 1/2005, de 5 de mayo, de la Comisión Permanente de la Junta Consultiva de Contratación Administrativa, ya estableció unas primeras recomendaciones y un modelo de cláusulas a tener en cuenta en el procedimiento de contratación en aquellos contratos que, habida cuenta de su objeto, puedan comportar el tratamiento de datos personales.

Pero ha sido la Ley 30/2007, de 30 de octubre, de contratos del sector público, en su disposición adicional trigésimo primera, la que ha incorporado por vez primera una referencia expresa a la protección de datos en la normativa de contratación pública. Además, ha previsto expresamente que en todos los casos en que la contratación implique el acceso del contratista a datos de carácter personal, de los que sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento y se tendrán que establecer las previsiones del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

En esta Recomendación se recogen los requisitos, el régimen jurídico, los efectos y las medidas de seguridad aplicables que se derivan de la existencia de un encargo de tratamiento de datos de carácter personal por cuenta de un tercero. Se recogen, no sólo las previsiones de la LOPD, sino también las derivadas de lo que se ha denominado el estatuto del encargado del tratamiento, recogido en el capítulo III del título II del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, y, especialmente, las que resultan de la mencionada disposición adicional trigésimo primera de la Ley 30/2007, de 30 de octubre, de contratos del sector público. Se recogen también las previsiones que se derivan del resto de la regulación del régimen jurídico de las administraciones públicas catalanas.

También se han tenido en cuenta dos documentos aprobados recientemente en el ámbito de la Unión Europea y que tienen una incidencia directa en el objeto de esta Recomendación: por una parte, la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países; por otra parte, el Dictamen 1/2010, del Grupo de Trabajo creado al amparo del artículo 29 de la Directiva 95/46/CE, sobre los conceptos de responsable del tratamiento y de encargado del tratamiento.

Este documento no pretende innovar el ordenamiento jurídico, sino hacer un recordatorio sistematizado de la normativa que afecta al encargado del tratamiento, por lo que respecta a su aplicación en el ámbito del sector público catalán e introducir recomendaciones para facilitar su cumplimiento.

Igualmente, en los anexos se ofrecen diferentes modelos de cláusulas para facilitar el cumplimiento de la normativa de protección de datos. Se distinguen aquellos supuestos en que los datos se traten en los locales del responsable del fichero o tratamiento, de aquéllos otros que se realicen en los locales del encargado del tratamiento y exclusivamente con sus medios. Estas cláusulas, que forman lo que en esta Recomendación denominaremos "contrato o acuerdo de encargo", pueden dar lugar a un contrato específico, se pueden incorporar en el mismo contrato o en cualquiera de los documentos que formen parte del mismo como anexos.

Se trata, en cualquier caso, de modelos orientativos que recogen las obligaciones derivadas de la normativa de protección de datos y también otras garantías que se consideran recomendables para una mejor protección del derecho, pero que habrá que ajustar a las circunstancias concretas de cada contrato.

De acuerdo con el artículo 15 del Estatuto de la Agencia Catalana de Protección de Datos, aprobado por Decreto 48/2003, de 20 de febrero, corresponde a la directora de la Agencia dictar las recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente en materia de protección de datos de carácter personal.

Por ello, con el informe previo favorable del Consejo Asesor de Protección de Datos de Cataluña y de la Junta Consultiva de Contratación Administrativa, dicto la siguiente

## RECOMENDACIÓN

### Capítulo 1

#### *Disposiciones generales*

#### 1

#### **Objeto**

1. El objeto de esta Recomendación es recoger, de forma sistematizada, los criterios a tener en cuenta desde el punto de vista de la protección de datos, en el momento de externalizar servicios que comporten el tratamiento de datos de carácter personal que sean responsabilidad de la entidad adjudicadora del contrato.

La Recomendación es aplicable, exceptuando el capítulo 3, a todos los contratos que comporten el tratamiento de datos de carácter personal. Afecta de una manera especial a los de gestión de servicios públicos y a los de servicios, pero también al

resto de contratos en que se lleve a cabo un tratamiento de datos por cuenta de la entidad adjudicadora.

También puede ser de aplicación, exceptuando el capítulo 2, al resto de acuerdos, convenios, delegaciones interadministrativas del ejercicio de competencias y encargos de gestión, incluidos los encargos a entes instrumentales de la Administración, que comporten el tratamiento de datos de carácter personal por cuenta de la entidad responsable.

2. En esta Recomendación también se ofrecen, en los anexos III a VI, modelos de cláusulas que recogen las obligaciones y previsiones convenientes para garantizar la protección de datos en la contratación o en el establecimiento de acuerdos con terceras entidades. Se trata, en cualquier caso, de modelos orientativos que deberán adecuarse a las peculiaridades de cada encargo, adaptándolos o introduciendo nuevas cláusulas, en especial las previstas en el apartado 7 de esta Recomendación.

**Normativa aplicable:** art. 15.1.e) Decreto 48/2003

2

## Ámbito de aplicación

La presente Recomendación se dirige a todos los órganos, organismos y entidades que forman parte o dependen de las instituciones públicas de Cataluña, de la Administración de la Generalidad, de los entes locales de Cataluña, de las universidades de Cataluña y del resto de entidades que forman parte del ámbito de actuación de la Agencia Catalana de Protección de Datos de acuerdo con el artículo 156 del Estatuto de Autonomía de Cataluña.

**Normativa aplicable:** arts. 3 Ley 5/2002; 156 EAC.

3

## Concepto de responsable del fichero o del tratamiento

Es responsable del fichero o del tratamiento la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, el contenido y el uso del tratamiento, aunque no lo realice materialmente.

También pueden ser responsables los entes sin personalidad jurídica que actúen en el tráfico jurídico como sujetos diferenciados.

**Normativa aplicable:** arts. 3.d) LOPD; 5.1.q) RLOPD.

4

## Concepto de encargado del tratamiento

1. Es encargado del tratamiento la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero o del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula y delimita su ámbito de actuación para la prestación de un servicio.

También pueden ser encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico jurídico como sujetos diferenciados.

2. Tiene la consideración de subencargado del tratamiento la persona, física o jurídica, que trate datos personales por encargo del encargado del tratamiento, y siempre por cuenta del responsable del fichero o tratamiento, en los supuestos y con los requisitos a los que se refiere el apartado 12 de esta Recomendación.

3. El tratamiento al que se refieren los apartados anteriores puede consistir en cualquier operación o procedimiento técnico, automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de datos, como también las cesiones que resulten de comunicaciones, consultas, interconexiones y transferencias. El encargo puede consistir directamente en realizar de forma exclusiva uno o más tratamientos o bien otras prestaciones que, de forma instrumental, comporten cualquier tratamiento de datos personales.

4. También puede existir encargo del tratamiento en aquellos casos en que no se produzca un acceso a datos que se encontraban previamente en poder del responsable del fichero, sino que en cumplimiento del encargo realizado los datos tengan que ser recogidos por el encargado.

5. El encargo puede ser a título gratuito o remunerado, ya sea directamente a través de una contraprestación a cargo del responsable, ya sea mediante la percepción de tasas, precios públicos u otros ingresos satisfechos por las personas usuarias.

6. El encargo puede establecerse por tiempo determinado o con carácter indefinido.

7. El encargo deberá formalizarse a través del contrato o acuerdo al que se refiere el apartado 6 de esta Recomendación.

**Normativa aplicable:** arts. 3.c) y g) LOPD; 5.1.i) y t) y 20.1 RLOPD.

## 5

### Elección del modelo organizativo

*Responsable:*

*Valore las implicaciones para la protección de datos en la elección de su modelo organizativo.*

Vistas las implicaciones que, en materia de protección de datos, puede tener la opción por uno u otro modelo organizativo (responsabilidad, titularidad pública o privada del fichero, régimen de comunicaciones, medidas de seguridad a implantar por cada una de las entidades implicadas, etc.), se recomienda que en el proceso de toma de decisión de la forma de gestión de un determinado servicio, o de la externalización de determinadas funciones que comporten el tratamiento de datos de carácter personal, se evalúen, como mínimo, los siguientes elementos:

- a) Si la prestación del servicio debe comportar el tratamiento de datos personales. En caso afirmativo, se recomienda identificar los datos que forman parte de la prestación del servicio y que, por lo tanto, deben sujetarse al encargo del tratamiento que se establezca.
- b) Si, en el caso de que la prestación de servicios no deba comportar el tratamiento de datos de carácter personal, se han previsto medidas para evitar cualquier tratamiento incidental de los datos.

- c) Si hay un fichero que recoja estos datos, debidamente creado e inscrito en el Registro de Protección de Datos de Cataluña. Si no es así, hay que crearlo previamente y notificar la creación al Registro de Protección de Datos de Cataluña.
- d) Si hay habilitación legal, o consentimiento de las personas afectadas, para la comunicación de datos al prestador del servicio o para la recogida y tratamiento por parte de éste. Si no hay habilitación legal y no se cuenta con el consentimiento de las personas afectadas, sólo se podrán comunicar los datos a la entidad prestadora de servicios si se ha formalizado el contrato o acuerdo de encargo establecido en el artículo 12 LOPD.
- e) Si hay normativa específica, por ejemplo en materia de salud o con respecto a las personas menores de edad que requiera determinadas condiciones para el tratamiento de la información. En caso de que la normativa específica exija algún determinado requisito, éste deberá tenerse en cuenta en el momento de seleccionar al encargado.
- f) Las medidas de seguridad que hay que exigir al contratista, de acuerdo con la normativa de protección de datos de carácter personal, en función de la naturaleza de los datos a tratar y de los riesgos previsibles. Hay que tener en cuenta el coste de implantación de las medidas a la hora de fijar el tipo de licitación o la contraprestación apropiada.
- g) Si los datos deben devolverse al responsable, si deben transferirse a otro encargado de tratamiento o si deben destruirse al finalizar la prestación.

El anexo I de esta Recomendación ofrece un esquema de los elementos a tener en cuenta en el proceso de toma de la decisión de encargar el tratamiento.

## 6

### El contrato o acuerdo de encargo del tratamiento

*Hay que suscribir el contrato o acuerdo de encargo previsto en el artículo 12 LOPD.*

1. El establecimiento de un encargo del tratamiento entre el responsable del fichero o tratamiento y terceras personas o entidades, a fin de que éstas lleven a cabo un tratamiento de datos personales por cuenta de aquél, deberá hacerse mediante un contrato o acuerdo de encargo con la forma a la que se refieren los apartados 9, 10 y 15 de esta Recomendación y con el contenido que se establece en el apartado siguiente.
2. La formalización de este contrato o acuerdo no requerirá el consentimiento de las personas afectadas. Tampoco será exigible, aunque puede ser recomendable, que se les informe expresamente sobre este extremo.
4. Sin perjuicio de lo que se establece en el apartado 8 de esta Recomendación con respecto a los contratos sometidos a la legislación de contratos del sector público, deberá establecerse, con carácter previo este acuerdo, si se quiere disfrutar de los efectos previstos en el artículo 12.1 de la LOPD, esto es, de la posibilidad de realizar comunicaciones de datos entre ambas entidades sin necesidad de consentimiento o de una ley específica que dé cobertura.

**Normativa aplicable:** art. 12 LOPD; 20 RLOPD.

*Deben incluirse en el contrato o acuerdo de encargo las previsiones legales y las recomendaciones del punto 2 de este apartado.*

1. De acuerdo con el artículo 12 de la LOPD, el contenido del contrato o acuerdo deberá prever expresamente:

- a) El compromiso del encargado del tratamiento de que no tratará los datos para una finalidad diferente de la que figure en el contrato o acuerdo de encargo.
- b) El compromiso del encargado del tratamiento de que tratará los datos de acuerdo con las instrucciones del responsable.
- c) El compromiso del encargado del tratamiento de que no los comunicará, ni siquiera para su conservación, a otras personas.
- d) Las medidas de seguridad que debe implementar el encargado del tratamiento.

El contenido del contrato no debe limitarse a una reiteración del enunciado del artículo 12.2 LOPD, sino que debe adaptar cada una de estas previsiones a la realidad de la prestación objeto de encargo.

2. No obstante, con el fin de dar cumplimiento al resto de obligaciones derivadas de la normativa de protección de datos se recomienda que en el contrato o acuerdo de encargo se haga referencia, si procede, a las siguientes cuestiones:

- a) Identificación del fichero o ficheros que incluyen los datos.
- b) Posibilidad de que durante la ejecución del encargo se comuniquen los datos a otro encargado del tratamiento.
- c) Otras cesiones que, en su caso, haya autorizado el responsable del tratamiento.
- d) Si, al final de la prestación, el encargado tiene que devolver los datos y los soportes o documentos donde consten, los debe entregar a otro encargado que designó el responsable o las tiene que destruir. En caso de destrucción, se recomienda prever también que el encargado tenga que acreditarla ante el responsable mediante un certificado.
- e) Obligación del encargado del tratamiento de dar cumplimiento al deber de información, en caso de que recoja los datos.
- f) Determinación del procedimiento de atención del ejercicio de los derechos de acceso, rectificación, cancelación y oposición, para el caso de que la solicitud se presente ante el encargado del tratamiento.
- g) La delegación, en su caso, al encargado del tratamiento, de la facultad de resolver los procedimientos de ejercicio de derechos.
- h) Posibilidad de subcontratación, en su caso, y si es posible, identificación del subcontratista.

- i) Autorización para tratar datos fuera de los locales del encargado o para tratarlos en dispositivos portátiles, si es necesario.
- j) Prohibición, en su caso, de incorporar los datos en soportes diferentes de los del responsable, en los supuestos en los que el encargado acceda a los datos remotamente.
- k) La delegación al encargado del tratamiento, en su caso, de la llevanza del documento de seguridad, cuando los datos se incorporen y se traten exclusivamente en los sistemas del encargado. En este caso, se recomienda también prever que el encargado tenga que entregar una copia del documento de seguridad al responsable.
- l) En los ficheros de nivel medio o alto, la comunicación al responsable del tratamiento de la designación del responsable de seguridad por parte del encargado del tratamiento.
- m) La comunicación, de forma inmediata, al responsable del tratamiento de las incidencias de seguridad que puedan afectar a la integridad o a la confidencialidad de los datos tratados.
- n) La delegación, en su caso, de las autorizaciones previstas en el título VIII del RLOPD, en relación con las medidas de seguridad.
- o) Los mecanismos previstos para verificar el cumplimiento, por parte del encargado, de las medidas de seguridad establecidas.
- p) El compromiso del encargado del tratamiento de formar al personal afectado sobre sus obligaciones derivadas de la normativa de protección de datos.
- q) Las otras instrucciones que el responsable considere convenientes.

3. En los anexos III y IV de esta Recomendación figuran modelos orientativos de cláusulas que se pueden incorporar en cualquiera de los documentos a los que se refieren los apartados 6, 9, 10 y 15 de esta Recomendación, adaptándolos a las circunstancias concretas de cada encargo, sin perjuicio de que cada entidad pueda incluir las cláusulas que se hayan previsto en el código tipo aplicable, en su caso, u otras que considere convenientes.

4. Se recomienda revisar todos los contratos, acuerdos y convenios existentes que impliquen el tratamiento de datos de carácter personal, con el fin de adecuarlos a estas previsiones. Si se debe incorporar o modificar alguna de estas previsiones, se podrá hacer mediante una modificación del contrato o acuerdo vigente o mediante un nuevo contrato o acuerdo debidamente formalizado.

**Normativa aplicable:** arts. 12.2 y 32 LOPD; 20.3, 21, 22, 26, 72, 82.1, 84, 86, 88.6, 89.2, 95 i 100 RLOPD.

## Capítulo 2

### *El encargado del tratamiento en la contratación del sector público*

*Hay que tener en cuenta la disposición adicional trigésimo primera de la Ley de contratos del sector público.*

1. De acuerdo con lo que establece la normativa de contratos del sector público, en cualquier contrato sometido a esta legislación que implique el acceso del contratista a datos de carácter personal de los que sea responsable la entidad adjudicadora, el contratista tendrá la consideración de encargado del tratamiento y deberá suscribir, necesariamente, las cláusulas a las que se refiere el apartado 7.1 de esta Recomendación.

2. En relación a los contratos que no estén sometidos a la normativa de contratación del sector público, el contratista que tenga que tratar datos de carácter personal por cuenta de la entidad contratante sólo tendrá la consideración de encargado del tratamiento si suscribe el contrato o acuerdo de encargo al que se refiere el apartado 6 de esta Recomendación.

**Normativa aplicable:** D.A. 31ª LCSP; art. 12 LOPD.

9

## **Pliegos de cláusulas administrativas y de prescripciones técnicas**

*Responsable:*

*Vele por que el contratista reúna las garantías necesarias para la protección de los datos personales.*

1. En la evaluación de la solvencia técnica de los licitadores en los contratos de servicios, en los de gestión de servicios públicos y en otros que comporten el tratamiento de datos de carácter personal se deberá velar por que el contratista reúna las garantías necesarias para dar cumplimiento a los principios y las garantías que prevé la normativa de protección de datos, en especial a las medidas de seguridad, sin perjuicio del resto de criterios que se puedan derivar de la legislación de contratos del sector público y de otra normativa sectorial.

En este sentido, cuando el tratamiento de datos por cuenta de la entidad adjudicadora sea un elemento relevante del contrato, puede ser recomendable prever la posibilidad de acreditar la solvencia técnica, con respecto al tratamiento de datos, mediante la acreditación de alguno de los certificados, sellos de calidad u otros documentos equivalentes, reconocidos en materia de protección de datos o de seguridad de la información.

2. En los pliegos de prescripciones técnicas o en el documento descriptivo de las especificaciones técnicas, deberán recogerse el sistema de tratamiento de la información, sus características y, en su caso, la concreción de las medidas de seguridad a aplicar.

3. Cuando el carácter sensible de los datos o el volumen de la información tratada así lo aconseje, se recomienda que estas circunstancias se tengan en cuenta en la determinación de los criterios de valoración de las ofertas y/o, en su caso, en la previsión de la posibilidad de presentar mejoras de la oferta, mediante la aplicación de medidas de seguridad complementarias a las exigibles de acuerdo con la normativa aplicable.

4. En los contratos de suministro de productos de software u otros elementos para el tratamiento de datos de carácter personal y en los contratos de servicios para la elaboración de software, se deberá incluir en el pliego de prescripciones técnicas el

nivel de seguridad, básico, medio o alto, que ha de permitir garantizar el nivel más alto de seguridad que corresponda en función de los datos que se prevean tratar.

**Normativa aplicable:** arts. 20.2 y D.A. RLOPD; 51 a 60, 99 a 102, 131, 134 y 165 LCSP.

10

## Forma del contrato o acuerdo de encargo

*Debe formalizarse por escrito el contrato o acuerdo de encargo entre ambas partes.*

1. En los contratos sometidos a la legislación de contratos del sector público, el acuerdo o contrato de encargo deberá constar necesariamente por escrito.
2. El acuerdo al que se refiere el apartado anterior podrá adoptar cualquiera de las formas siguientes:
  - a) Un contrato o acuerdo específico.
  - b) Cláusulas específicas incluidas en el contrato adjudicado, si procede mediante un anexo.
  - c) Cláusulas específicas incluidas en el pliego de cláusulas administrativas particulares.
  - d) Cláusulas específicas incluidas en el pliego de prescripciones técnicas.
3. Cuando se trate de supuestos no sometidos a la legislación de contratos del sector público, se recomienda dejar constancia igualmente por escrito, aunque la relación entre el responsable y el encargado del tratamiento puede constar también en alguna otra forma que permita acreditar la suscripción del mismo y su contenido.
4. El contrato o acuerdo de encargo del tratamiento deberá suscribirlo el responsable del fichero o un superior jerárquico de éste que tenga la condición de órgano de contratación.

**Normativa aplicable:** D.A. 31ª, 99, 100, 140 y 192 LCSP.

11

## Contratos menores

*Debe formalizarse el contrato o acuerdo de encargo también en los contratos menores.*

En los contratos menores que comporten el tratamiento de datos personales por cuenta del responsable del fichero o del tratamiento, se requiere igualmente la formalización del acuerdo al que se refiere el apartado anterior.

**Normativa aplicable:** 95 y D.A. 31ª LCSP.

12

## Subcontratación

**Encargado:** *Subcontrate sólo en los supuestos previstos en la normativa de contratación pública.*

1. Sin perjuicio de que el encargado del tratamiento pueda contratar con terceros en nombre y por cuenta del responsable del fichero o del tratamiento con su autorización, el encargado del tratamiento podrá subcontratar con un tercero, que tendrá la condición de subencargado, parte de la prestación encargada que conlleve el tratamiento de datos personales, siempre que se cumplan los siguientes requisitos:

- a) Que la posibilidad de subcontratar el tratamiento o tratamientos se haya especificado en el contrato o en el pliego de cláusulas administrativas particulares. Si no se ha previsto y durante la prestación del servicio se pretende subcontratar, debe modificarse el contrato que se haya suscrito, con el fin de prever esta posibilidad.
- b) Que se haya identificado en el contrato la empresa o empresas subcontratistas, o que se comunique previamente al responsable del tratamiento.
- c) Que el subcontratista se ajuste a las instrucciones del responsable del fichero o tratamiento.
- d) Que se formalice un contrato o acuerdo de encargo entre el encargado del tratamiento y el subencargado.

2. En los contratos, convenios y acuerdos que no estén sometidos a la normativa de contratación de las administraciones públicas, sólo se podrá subcontratar el tratamiento de datos personales en los supuestos y con los requisitos previstos en el artículo 21 RLOPD a los que se refiere el apartado 17 de esta Recomendación.

3. Cuando el subencargado cumpla los requisitos previstos en los números anteriores, se considerará encargado del tratamiento, y le será de aplicación el régimen jurídico aplicable a éste.

**Normativa aplicable:** apartado 3 D.A. 31ª LCSP; 21 RLOPD.

13

### **Ejecución de contratos que no requiera el acceso a datos personales**

*Responsable:* *Prevea las medidas necesarias para evitar accesos indebidos.*

En los contratos que no deban comportar el acceso por terceros a datos de carácter personal, como, por ejemplo, los contratos de limpieza, seguridad o mantenimiento general, entre otros, la empresa contratista no tiene la condición de encargado del tratamiento.

No obstante, cuando, a pesar de no tratarse datos de carácter personal, el prestador pueda entrar en contacto con los documentos o soportes donde estén almacenados, el contrato deberá recoger expresamente la prohibición de acceder a datos personales y el deber de secreto si, de forma incidental, aquél tiene acceso.

En estos casos, se recomienda incluir en el contrato con estas empresas una cláusula similar a la que figura en el anexo V de esta Recomendación y aplicar las medidas de seguridad a las que se refiere el apartado 38 de esta Recomendación.

**Normativa aplicable:** art. 83 RLOPD.

## **Capítulo 3**

*El encargado del tratamiento en convenios, delegaciones interadministrativas, encargos de gestión y otras fórmulas análogas*

## Utilización de la figura del encargado del tratamiento

*Responsable: Valore la posibilidad de suscribir acuerdos de encargo del tratamiento.*

En el establecimiento de convenios, delegaciones interadministrativas o encargos de gestión que impliquen, para una de las partes, el tratamiento de datos de carácter personal de los que sea responsable la otra parte del convenio, delegación o encargo de gestión, se podrá establecer el acuerdo al que se refiere el apartado 6 de esta Recomendación. En este caso la entidad que trate los datos por cuenta de la otra administración tendrá la consideración de encargado del tratamiento.

Igualmente, también se podrá establecer el mencionado acuerdo con los entes instrumentales, de naturaleza pública o privada, que creen las administraciones públicas catalanas para el ejercicio de las funciones o la gestión de los servicios que tengan atribuidos. En este caso el ente instrumental tendrá la consideración de encargado del tratamiento y la administración de la que depende seguirá manteniendo la titularidad del fichero.

**Normativa aplicable:** arts. 3.g y 12 LOPD; 6, 13, 15 LRJPAC; 9, 137 y ss, 150, 153 y 191 TRLMRLC; 303 y ss. ROAS.

## Acuerdo de encargo del tratamiento de datos

*Hay que formalizar el encargo de tratamiento de datos personales.*

Cuando el encargo derive de la existencia de un convenio o encargo de gestión, el acuerdo al que se refiere el apartado 6 de esta Recomendación deberá formalizarse en el mismo convenio o mediante un acuerdo específico.

Cuando se trate de delegaciones de competencias, el contenido del acuerdo podrá incorporarse al acto administrativo en el que se produzca la delegación. En cualquier caso, quedará sometido a la aceptación por parte de la entidad delegada.

Cuando se trate de entes instrumentales, el contenido del acuerdo podrá incluirse en el convenio marco, contrato programa, acuerdo o cualquier otro instrumento que regule las relaciones entre el ente instrumental y la administración de la que depende.

**Normativa aplicable:** art. 12 LOPD.

## Transmisiones intradministrativas de datos

*Pueden aplicarse las garantías del encargo del tratamiento también a las transmisiones intradministrativas de datos.*

De acuerdo con la normativa de protección de datos se considera comunicación toda revelación de datos realizada a una persona diferente de la persona interesada. Por ello, de acuerdo con la normativa de protección de datos, las transmisiones de datos entre órganos que forman parte de una misma administración no se considerarán una

comunicación de datos y, por lo tanto, no será necesaria la formalización del contrato o acuerdo de encargo al que se refiere el apartado 6 de esta Recomendación, al efecto de comunicarle los datos, sin perjuicio del obligado cumplimiento del principio de finalidad.

No obstante, en estos casos se recomienda igualmente que, con carácter previo a la comunicación, el responsable del fichero o tratamiento recuerde al órgano destinatario de la información la necesidad de cumplir con el deber de confidencialidad, las medidas de seguridad aplicables y el resto de extremos a los que se refiere el apartado 7.1 de esta Recomendación.

**Normativa aplicable:** arts. 3.i) LOPD; 5.1.c) RLOPD.

17

## Subencargo del tratamiento

*Sólo hay que utilizar el subencargo del tratamiento en los supuestos previstos en el artículo 21 del RLOPD.*

1. El encargado del tratamiento sólo podrá encargar el tratamiento, o una parte de éste, a un tercero en los siguientes supuestos:

a) Cuando haga el subencargo en nombre y por cuenta del responsable del tratamiento, con la autorización de éste último.

b) Cuando se cumplan los tres requisitos siguientes:

- 1) Que se especifiquen en el contrato o acuerdo de encargo los servicios que puedan ser objeto de subencargo y, si es posible, la empresa con la que se tiene que subcontratar. Si no es posible identificar a la empresa en el contrato, es necesario que el encargado del tratamiento comunique al responsable los datos de la empresa con carácter previo al subencargo.

Cuando no se haya previsto en el contrato o acuerdo de encargo, si con posterioridad resulta necesario hacer un subencargo, se tiene que someter al responsable esta cuestión, y obtener su autorización.

- 2) Que el tratamiento por parte del subencargado se ajuste a las instrucciones del responsable del fichero.
- 3) Que se formalice un contrato o acuerdo de encargo entre el encargado del tratamiento y el subencargado.

2. Cuando el subencargado cumpla los requisitos previstos en el número anterior, se considerará encargado del tratamiento, y le será de aplicación el régimen jurídico aplicable a éste.

**Normativa aplicable:** art.21 RLOPD.

## Capítulo 4

### *Efectos de la existencia de un encargo del tratamiento*

*Hay que identificar claramente los ficheros afectados por el encargo.*

1. El encargado del tratamiento está sujeto a los principios y garantías que establece la normativa de protección de datos de carácter personal.
2. Se recomienda identificar con la máxima precisión posible el fichero o ficheros afectados por el encargo en el momento de formalizar el contrato o acuerdo de encargo.
3. Cuando el encargado del tratamiento gestione otros datos por cuenta propia, o en virtud de otros encargos, los efectos del encargo del tratamiento se limitarán a los tratamientos de datos que se lleven a cabo como consecuencia de la ejecución de cada encargo.

El encargo del tratamiento no afecta a los tratamientos que se deriven de los ficheros propios de que disponga el encargado para su funcionamiento, como son los relativos a su personal, proveedores, etc., salvo que se destinen exclusivamente al cumplimiento del servicio encargado, que sean de la responsabilidad del ente que formula el encargo y que así se haya establecido en el contrato o acuerdo de encargo.

**Normativa aplicable:** art.12 LOPD.

*Debe verificarse la legitimación para llevar a cabo el encargo.*

El tratamiento de datos de carácter personal efectuado por el encargado del tratamiento encuentra legitimación en aquellas circunstancias previstas en el artículo 6 de la LOPD que den legitimación al responsable del fichero o tratamiento, siempre que se haya establecido el correspondiente acuerdo con el contenido previsto en el apartado 7.1 de esta Recomendación.

**Normativa aplicable:** arts. 6 y 12 LOPD.

*Encargado: Informe en el momento de la recogida de datos.*

Cuando el tratamiento efectuado por el encargado comporte que éste lleve a cabo la recogida de datos de carácter personal que pasen a formar parte de los ficheros del responsable, el encargado también deberá hacerse cargo del deber de información que establece el artículo 5 de la LOPD, salvo que se haga cargo el responsable.

A tal efecto, en el Anexo VI de esta Recomendación se incluye un modelo de cláusula informativa a fin de que el encargado del tratamiento pueda cumplir con este deber.

A pesar de que, a efectos del artículo 5.1.a) de la LOPD, la comunicación de datos al encargado no tiene la consideración de comunicación de datos, cuando los datos se traten en los sistemas del encargado se recomienda informar sobre la existencia de unos o más encargados del tratamiento y, en su caso, identificarlos.

**Normativa aplicable:** art.5 LOPD.

21

## Vinculación a la finalidad

**Encargado:** *Utilice los datos sólo para la finalidad del encargo.*

Los datos recibidos o recogidos al amparo de un encargo del tratamiento no se pueden utilizar para otras finalidades diferentes a las del encargo, salvo que una norma con rango legal imponga esta obligación o se cuente con el consentimiento de las personas afectadas.

**Normativa aplicable:** arts. 4 y 12 LOPD; 20.3 RLOPD.

22

## Instrucciones del responsable del fichero o tratamiento

**Responsable:** *Deje constancia por escrito de las instrucciones que debe seguir el encargado del tratamiento.*

El responsable del fichero o tratamiento, en el contrato o acuerdo de encargo, o después de formalizarlo, podrá dar al encargado las instrucciones que considere necesarias en relación con los tratamientos que se deriven del objeto del encargo. En el caso incumplir estas instrucciones, el encargado también se considerará responsable de las posibles infracciones en que se incurra.

Aunque la normativa de protección de datos no exige expresamente que las instrucciones se den por escrito, se recomienda hacerlo de manera que quede constancia, mientras no hayan prescrito las posibles responsabilidades.

**Normativa aplicable:** arts. 12 LOPD; 20.3 RLOPD.

23

## Deber de confidencialidad

**Encargado:** *Respete el deber de confidencialidad.*

1. El encargado del tratamiento está sujeto al deber de confidencialidad con respecto a los datos de carácter personal de los que tenga conocimiento en virtud del encargo.

2. El deber de confidencialidad se mantendrá una vez finalizada la relación con el responsable del fichero.

**Normativa aplicable:** arts. 10 y 12 LOPD; 20.3 RLOPD.

24

## Régimen de comunicaciones

**Encargado:** *Limite la comunicación de datos a los supuestos legalmente habilitados.*

1. En los supuestos de tratamiento de datos por cuenta del responsable en los que se haya suscrito el contrato o acuerdo de encargo con el contenido al que se refiere el apartado 7.1 de esta Recomendación, no será necesario el consentimiento de las personas afectadas para llevar a cabo las comunicaciones de datos entre el responsable del fichero o tratamiento y el encargado del tratamiento, o viceversa, siempre que tengan por objeto el cumplimiento del encargo.

2. El encargado del tratamiento no podrá comunicar a ningún otro destinatario los datos a los que haya tenido acceso en la ejecución del contrato, o los que haya elaborado a partir de éstos, con independencia de que los pliegos de cláusulas o el contrato hayan o no previsto el carácter confidencial, salvo en los siguientes supuestos:

a) Cuando se haya establecido en el contrato o acuerdo que, al finalizar el encargo, el encargado debe entregar los datos al nuevo encargado que el responsable designe. También podrá hacerlo cuando, a pesar de que el contrato o acuerdo prevea que los datos deben devolverse al responsable, éste dé instrucciones al encargado a fin de que entregue los datos al nuevo encargado.

b) En los supuestos de subcontratación, de acuerdo con lo establecido en la disposición adicional 31ª de la Ley de Contratos del Sector Público (véase apartado 12 de esta Recomendación) o en el artículo 21 RLOPD (véanse apartados 12.2 y 17 de esta Recomendación).

c) Cuando la posibilidad de comunicación se haya previsto en el contrato o acuerdo, o el responsable le autorice y se cuente con el consentimiento de la persona titular de los datos o con la habilitación de una norma legal. En estos casos, se recomienda prever las medidas de seguridad adicionales apropiadas para llevar a cabo las comunicaciones.

**Normativa aplicable:** arts. 11 y 12 LOPD; 20.3 y 22.1 RLOPD.

25

## Encargos que impliquen transferencias internacionales de datos

*Deben incluirse también las cláusulas adecuadas cuando se transfieran datos a encargados ubicados en países que no ofrezcan un nivel adecuado de protección.*

Cuando la transmisión de datos al encargado implique una transferencia internacional de datos a países que no formen parte de la Unión Europea y respecto de los cuales la Comisión Europea o la Agencia Española de Protección de Datos no haya declarado que ofrecen un nivel adecuado de protección, será necesario que la Agencia Española de Protección de Datos autorice dicha transferencia.

A efectos de obtener la autorización, el responsable podrá ofrecer garantías suficientes, con respecto a la protección de datos, a través de la inclusión de cláusulas contractuales adecuadas. Con esta finalidad, conviene tener en cuenta las cláusulas contractuales tipo contenidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero, en cumplimiento de lo establecido en el artículo 26.4 de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos.

**Normativa aplicable:** arts. 33 y 34 LOPD; 70 RLOPD; Decisión 2010/87/UE, de 5 de febrero.

26

## Notificación al Registro de Protección de Datos de Cataluña

*Responsable:*

*Notifique la existencia de encargado del tratamiento cuando el fichero se ubique en sus dependencias.*

1. Corresponde al responsable del fichero crear el fichero, así como notificar la creación, modificación y supresión al Registro de Protección de Datos de Cataluña.
2. La existencia de uno o diversos encargados del tratamiento no hace falta que se incluya en la disposición general o acuerdo de creación del fichero. No obstante, cuando el fichero se ubique en las dependencias o instalaciones del encargado del tratamiento, deberá indicarse la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición ante éste o ante el responsable. En este caso, en la notificación del fichero al Registro deberá identificarse el encargado del tratamiento en el formulario que se puede encontrar en la web de la Agencia ([www.apd.cat](http://www.apd.cat)). Igualmente deberán comunicarse al Registro de Protección de Datos de Cataluña los cambios de encargado del tratamiento que se produzcan.

**Normativa aplicable:** arts. 20 y 26.1 LOPD; 26 y 55.2 RLOPD.

27

## Ejercicio de derechos

*Deben adoptarse medidas para facilitar el ejercicio de derechos.*

1. Corresponde al responsable del fichero atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Cuando la solicitud se haya presentado ante el encargado del tratamiento, éste debe comunicarlo al responsable del fichero lo antes posible, de acuerdo con el procedimiento que se haya establecido en el contrato o acuerdo, a fin de que el responsable pueda resolverla dentro del plazo establecido.
2. No obstante, en el contrato o acuerdo de encargo, el responsable del fichero puede delegar en el encargado del tratamiento la resolución de los procedimientos de ejercicio de estos derechos.

En el anexo II de esta Recomendación figura un cuadro ilustrativo del proceso de toma de decisión en relación con el procedimiento para atender las solicitudes de ejercicio de derechos, en los casos en que exista la figura del encargado del tratamiento.

**Normativa aplicable:** art. 26 RLOPD.

*Hay que concretar en el contrato o acuerdo de encargo el destino final de los datos.*

1. Finalizada la prestación y, en el caso de los contratos, antes del acto formal de recepción o de conformidad con la realización del objeto del contrato, deberán devolverse o destruirse los datos, los soportes y los documentos donde aquéllos consten, de acuerdo con lo que se haya establecido en el contrato o acuerdo. Esta previsión se refiere tanto a los datos que inicialmente le haya comunicado el responsable, como a los datos que haya elaborado a partir de aquéllos o los que el encargado haya recogido posteriormente por cuenta de aquél.

La decisión de si hace falta o no devolver los datos corresponde al responsable. Por lo tanto, se recomienda evitar la utilización de cláusulas que no concreten este extremo o lo dejen a la decisión del encargado del tratamiento.

2. La devolución deberá hacerse al responsable o, si se ha establecido en el contrato o así lo indica el responsable, al nuevo encargado del tratamiento que el responsable haya designado.

3. En ningún caso se podrán destruir los datos cuando sean necesarios para garantizar la continuidad de la prestación de un servicio público, o cuando alguna otra previsión legal exija la conservación.

4. Los ficheros temporales o las copias que se entreguen al encargado deberán destruirse cuando dejen de ser necesarios para el cumplimiento de la prestación encargada.

5. Cuando la información se haya tratado mediante equipos informáticos, hay que asegurarse, mediante los procedimientos técnicos adecuados, del borrado total de los datos personales tratados, de manera que no se puedan recuperar o reconstruir.

6. Cuando proceda la destrucción de los documentos o soportes en los que se hayan almacenado los datos, como CD, conviene destruirlos mediante máquinas destructoras que impidan su reutilización o reconstrucción.

7. Se recomienda prever que, una vez destruidos los datos, el encargado tenga que certificar por escrito la destrucción y que este certificado se envíe al responsable del fichero.

8. En cualquiera de los casos expuestos, el encargado del tratamiento podrá conservar una copia de los datos, debidamente bloqueados, con el fin de atender las posibles responsabilidades derivadas del tratamiento, mientras estas responsabilidades no hayan prescrito. Una vez transcurrido este plazo, debe destruir las copias.

**Normativa aplicable:** arts. 4.5 y 12.3 LOPD; 22, 92.4 y 105.2.d) RLOPD.

*Encargado: Hay que tener en cuenta las responsabilidades en que se puede*

1. El encargado del tratamiento está sujeto al cumplimiento de todos los principios y garantías de la LOPD. Por lo tanto, está sujeto al régimen de responsabilidad civil o responsabilidad patrimonial de la Administración por los daños o lesiones que sufran las personas interesadas como consecuencia del incumplimiento de lo establecido en la normativa de protección de datos.

2. Con respecto al régimen sancionador previsto en la normativa de protección de datos, y sin perjuicio de las responsabilidades en que pueda incurrir el responsable del fichero o tratamiento, el encargado del tratamiento también se considerará responsable del tratamiento en los siguientes supuestos:

- a) Cuando destine los datos a otra finalidad, salvo que una norma con rango legal lo establezca como obligación, o bien se cuente con el consentimiento de las personas afectadas.
- b) Cuando comunique los datos, salvo que:
  - a. Las instrucciones del responsable prevean la comunicación.
  - b. El responsable ordene la comunicación a un tercero, que también tenga la condición de encargado del tratamiento del mismo responsable.
  - c. Se trate de uno de los supuestos de subcontratación legalmente admitidos.
- c) Cuando utilice los datos incumpliendo las estipulaciones del contrato o acuerdo de encargo.
- d) Cuando no implante las medidas de seguridad estipuladas en el contrato o acuerdo de encargo.

3. El régimen sancionador previsto en la LOPD es independiente y compatible con el régimen de penalidades que, en uso de la facultad prevista en el artículo 196.1 de la Ley de contratos del sector público, se hayan previsto en el contrato.

**Normativa aplicable:** arts. 12.4, 19 y 43 LOPD; 16 Ley 5/2002; 20.3 RLOPD; 196.1 LCSP.

## Capítulo 5

### *Medidas de seguridad*

30

#### **Medidas de seguridad aplicables**

*Hay que prever e implantar las medidas de seguridad legalmente exigibles, adaptadas al objeto de encargo.*

1. El encargado del tratamiento deberá aplicar las medidas de seguridad previstas en la normativa de protección de datos, de acuerdo con el nivel que corresponda aplicar a cada uno de los ficheros en función de los datos que se traten en cada caso y de las medidas adicionales que haya establecido el responsable del tratamiento, sin perjuicio de otras medidas que puedan exigibles de acuerdo con el resto de normativa aplicable. Ello sin perjuicio de que el responsable del tratamiento tenga que cumplir también estas medidas en la parte que le corresponda.

2. Cuando un mismo sistema de información incluya información sobre diversos encargos, se recomienda adoptar medidas específicas para asegurar que los datos se utilizarán sólo con la finalidad para la cual se recogieron.

**Normativa aplicable:** arts.10 y 12.2.2 LOPD; 79 y 82.3 RLOPD.

*Hay que verificar que el encargado cumple con la normativa de protección de datos.*

1. Cuando el tratamiento se lleve a cabo en los locales del encargado o mediante sus sistemas, el encargado deberá someterse a las auditorías que lleve a cabo el responsable del fichero o tratamiento, directamente o a través de un tercero a quien se le haya encargado, y deberá colaborar con el fin de comprobar la aplicación de las medidas de seguridad exigibles y el cumplimiento del resto de principios y garantías en materia de protección de datos.

2. Sin perjuicio del deber de auditoría bienal previsto en la normativa de protección de datos para los ficheros de nivel medio o alto, cuando el encargo tenga una duración superior a un año se recomienda prever en el contrato o acuerdo que estas auditorías se llevarán a cabo al inicio de la prestación del servicio y, como mínimo, una vez cada dos años, cualquiera que sea el nivel aplicable.

**Normativa aplicable:** arts. 20.2 y 96 RLOPD.

*Responsable: Supervise el acceso del encargado a sus ficheros.*

1. Cuando el tratamiento de datos de carácter personal se realice en los locales del responsable, deberá constar en el documento de seguridad de éste que el encargado del tratamiento puede acceder a los datos.

2. Si los datos se encuentran en los sistemas del responsable y el encargado accede remotamente, el acceso deberá someterse a las medidas de seguridad establecidas en la normativa de protección de datos y deberá garantizar un nivel de seguridad equivalente al que corresponda a los accesos en modo local. Si se le ha prohibido la incorporación de los datos en soportes diferentes de los del responsable, también deberá constar en el documento de seguridad del responsable.

3. En cualquiera de estos casos, el encargado debe velar por que su personal cumpla con las medidas de seguridad que figuren en el documento de seguridad del responsable.

**Normativa aplicable:** arts. 82.1 y 89.2 RLOPD.

*Encargado: Adapte su documento de seguridad al encargo recibido o elabore uno específico.*

Cuando los datos se traten en sus locales, el encargado del tratamiento deberá tener en cuenta, en su documento de seguridad, las implicaciones derivadas del encargo recibido.

No obstante, se recomienda aprobar un documento de seguridad, si procede común, para todos los tratamientos que se realicen en sus locales donde actúe como encargado, que sea diferente del aplicable a sus propios ficheros.

**Normativa aplicable:** arts. 88.2 y 88.5 RLOPD.

34

## Documento de seguridad del responsable

**Responsable:** *Compruebe que el documento de seguridad contenga las previsiones necesarias de acuerdo con el objeto del encargo.*

1. El documento de seguridad del responsable deberá prever:

a) Cuando se presten los servicios en los locales del responsable:

- a. Ficheros o tratamientos afectados por el encargo.
- b. Identificación del encargado del tratamiento, con indicación del contrato o acuerdo de encargo y su vigencia.
- c. Régimen de acceso a los datos por parte del encargado del tratamiento.
- d. Autorización, en su caso, para que el encargado pueda almacenar datos en dispositivos portátiles o tratarlos fuera de los locales del responsable.
- e. Prohibición, en su caso, de incorporar los datos en soportes diferentes de los del responsable, en los supuestos en que el encargado tenga acceso remoto.
- f. El resto de aspectos establecidos en el RLOPD.

b) Cuando se presten los servicios en los locales del encargado:

- a. Ficheros o tratamientos afectados por el encargo.
- b. Identificación del encargado, con indicación del contrato o acuerdo de encargo y su vigencia.
- c. Cuando el tratamiento se realice exclusivamente con los sistemas del encargado, debe anotarse esta circunstancia.
- d. Habilitación, en su caso, y requisitos para que el encargado del tratamiento pueda autorizar el almacenamiento de datos en dispositivos portátiles o que se traten fuera de los locales del encargado.
- e. El resto de aspectos establecidos en el RLOPD.

2. Cuando los datos se traten exclusivamente en los sistemas del encargado, la llevanza del documento de seguridad del responsable se podrá delegar en el encargado del tratamiento, mediante el contrato o convenio que regule el encargo.

**Normativa aplicable:** arts. 82, 86 y 88 RLOPD.

35

## Documento de seguridad del encargado

**Encargado:** *Adapte también, en su caso, su documento de seguridad.*

Sin perjuicio de lo que establece el número 2 del apartado anterior, cuando el encargado trate la información en sus locales o sistemas, deberá cumplir lo que se

establezca en el documento de seguridad del responsable o responsables y, en su caso, adaptar su propio documento de seguridad.

A estos efectos, se recomienda que el documento de seguridad del encargado prevea:

- a) Los ficheros o tratamientos que se traten en concepto de encargado.
- b) La referencia expresa al contrato o documento que regula el encargo.
- c) La identificación de la persona responsable.
- d) El periodo de vigencia del encargo.
- e) Las medidas de seguridad a implantar por el encargado derivadas del documento de seguridad del responsable o responsables. También aquellas otras que resulten convenientes, visto el volumen de información que acabe tratando o bien por la acumulación, en los mismos sistemas, de información proveniente de diversos responsables o del mismo encargado.
- f) Cuando preste los servicios en sus propios locales, la autorización, en su caso, de los usuarios que puedan almacenar datos en dispositivos portátiles o tratarlas fuera de sus locales.
- g) El resto de aspectos establecidos en el RLOPD.

**Normativa aplicable:** arts. 82.2, 86 y 88 RLOPD

36

### Responsable de seguridad

**Encargado:**

*Designe también a un responsable de seguridad cuando la información se trate en sus sistemas.*

Con independencia de que la normativa de protección de datos exija al responsable del fichero la designación de un responsable de seguridad para los ficheros en los que se deben aplicar medidas de nivel medio o alto, cuando los datos personales se incorporen en los sistemas del encargado, se recomienda que, en estos supuestos, éste también designe a una persona que sea responsable de la implantación de las medidas de seguridad y de inspección, con el fin de comprobar su efectividad. Cuando así se establezca en el contrato o acuerdo de encargo, la designación y el perfil profesional de la persona designada deberán comunicarse al responsable del fichero.

**Normativa aplicable:** arts. 82, 86 y 88 RLOPD

37

### Delegación de autorizaciones

**Responsable:**

*Valore la posibilidad de delegar en el encargado las autorizaciones en materia de seguridad.*

Las autorizaciones que la normativa de protección de datos atribuye al responsable del fichero o tratamiento en materia de medidas de seguridad se podrán delegar en el encargado del tratamiento cuando afecten a partes del tratamiento que formen parte del encargo.

**Normativa aplicable:** art. 84 RLOPD.

*Evite accesos indebidos.*

1. En las prestaciones de servicios por terceros que no deban comportar el acceso a datos de carácter personal, como, por ejemplo, contratos de limpieza, seguridad, mantenimiento general u otros, el responsable del fichero o tratamiento deberá informar al personal que intervenga en la prestación de servicios sobre los riesgos que puede generar su actividad para el sistema de información, así como sobre otros aspectos como el sistema de control de los accesos físicos, el proceso de eliminación de documentos y soportes o las condiciones de ventilación y refrigeración necesarias para el correcto funcionamiento de los equipos.

En cualquier caso, el responsable del fichero o tratamiento deberá adoptar las medidas de seguridad adecuadas para limitar la posibilidad de que el personal de estas empresas acceda a los datos de carácter personal.

2. Se recomienda incluir en el contrato de prestación de servicios la obligación de la entidad adjudicataria de poner en conocimiento del responsable del fichero o tratamiento, de forma inmediata, cualquier incidencia que se produzca durante la prestación del servicio que pueda afectar a la integridad o a la confidencialidad de los datos de carácter personal tratados por la entidad adjudicadora.

3. Se recomienda aplicar estas medidas, también, por los encargados del tratamiento que subcontraten con terceras empresas prestaciones que no hayan de comportar el acceso a datos de carácter personal.

**Normativa aplicable:** art. 83 RLOPD.

Barcelona, 6 d'abril de 2010

Esther Mitjans Perelló  
Directora

## Abreviaturas

**EAC:** Estatuto de Autonomía de Cataluña.

**LOPD:** Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

**LCSP:** Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

**LRJPAC:** Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

**RLOPD:** Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

**Ley 5/2002:** Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

**TRLMRLC:** Texto refundido de la Ley Municipal y de régimen Local de Cataluña, aprobado por el Decreto legislativo 2/2003, de 28 de abril.

**ROAS:** Reglamento de obras, actividades y servicios de los entes locales, aprobado por el Decreto 179/1995, de 13 de junio.