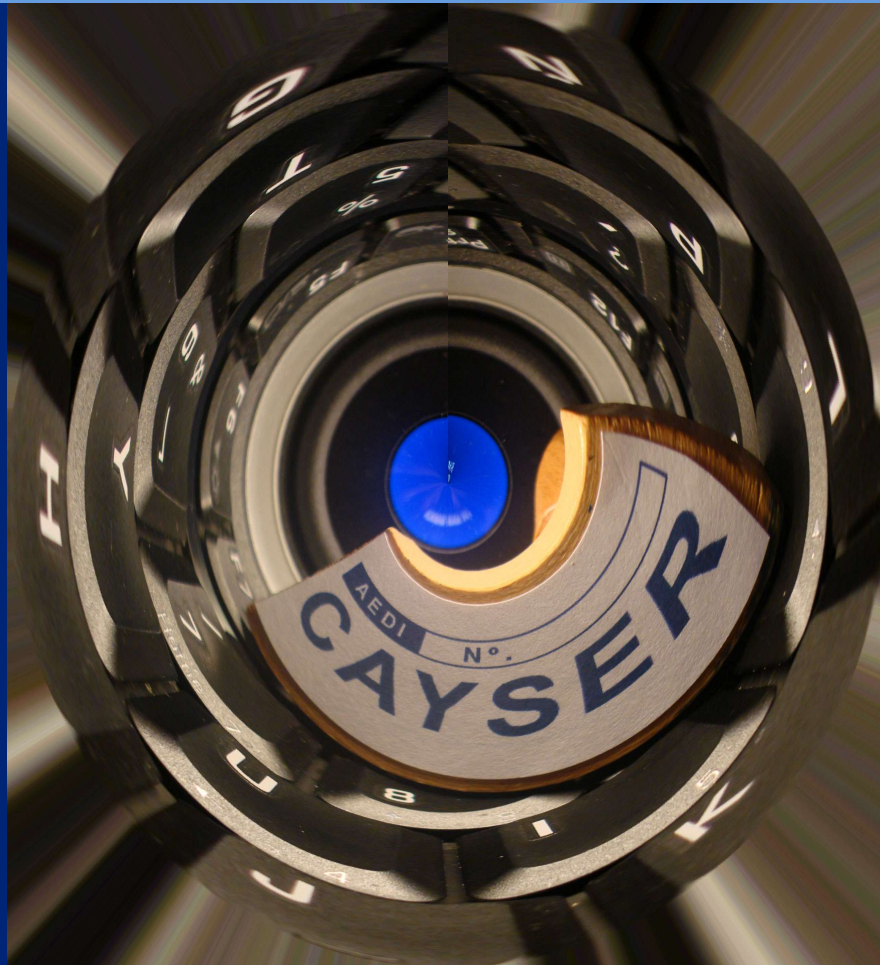


Certificación Oficial de Calidad de Servicio TIC

AEDI **CAYSER**

Informe de la Agencia Española de Protección de Datos
Personales para la aplicación de la Certificación "AEDI
CAYSER 2071-ES", de 23-Marzo-2007



AEDI

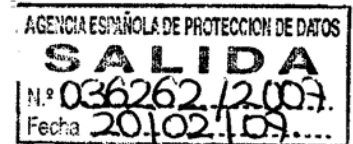


Asociación
Española para la
Dirección
Informática

c/. Padre Damián nº 40, 1º 28036 Madrid España
Tfno. 902.152.407 - Fax 902.152.408 - www.aedi.es



Nº Refª.: 100196/2006



D. Alfredo Izquierdo
Vicepresidente
Asociación Española para la Dirección Informática
C/ Padre Damián, 40 – 1º
28036 - MADRID

En contestación a su escrito de fecha 25 de octubre de 2006, con registro de entrada en esta Agencia el 30 de octubre, adjunto informe elaborado al efecto por nuestro Gabinete Jurídico.

Debo significar que el mismo no tiene carácter vinculante y no prejuzga el criterio del Director de la Agencia en el ejercicio de sus funciones, entre las que la Ley no prevé la evacuación de consultas vinculantes.

Madrid, 19 de febrero de 2007

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCION DE DATOS

Fdo.: José Luis Piñar Mañas

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos personales necesarios para dar respuesta a la consulta planteada han sido incorporados al fichero "Consultas" del que es responsable la Agencia Española de Protección de Datos, creado por la Resolución del Director de la Agencia de fecha 27 de julio de 2001 (B.O.E. de 17 de agosto de 2001), con la finalidad de poder tramitar su solicitud y remitirle el correspondiente informe. Ud. podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante la Agencia Española de Protección de Datos, calle Jorge Juan 6, 28001 Madrid.



Ref. de entrada 100196/2006 (Asociación Española para la Dirección Informática)

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por la Asociación Española para la Dirección Informática, cúmpleme informarle lo siguiente:

La consulta plantea la adecuación a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, del texto que se remite relativo a la normativa de la Marca de Garantía Oficial de Calidad de Servicios TIC que denominan "AEDI CAYSER", en aquellos aspectos que revisten trascendencia en lo que a la protección de datos de carácter personal se refiere.

Como cuestión previa, debe recordarse que el artículo 2.1, párrafo primero de la Ley Orgánica 15/1999 dispone que "la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", siendo datos de carácter personal, conforme al artículo 3 a) "Cualquier información concierne a personas físicas identificadas o identificables".

Quiere ello decir que, la protección conferida por la Ley Orgánica 15/1999 no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran exigirse en el caso de que el uso de información relativa a las empresas les cause algún perjuicio, si bien sí sería de aplicación la Ley en caso de que la información se refiriera no sólo a la empresa, sino a una determinada persona física que preste sus servicios en la misma (considerada, por ejemplo, persona de contacto).

En consecuencia, el contenido de este informe se centrará en analizar las implicaciones que, en materia de protección de datos de carácter personal, puede suponer la actividad que se describe en la consulta, es decir el tratamiento de datos de carácter personal en el texto que se remite.

En este sentido, procede realizar las siguientes observaciones:



I

En el capítulo 4º relativo al Registro Histórico de Información al Cliente, aparecen relacionados los datos que deben contener estos registros entre los que se citan los referidos la "persona de contacto con el cliente" y el "responsable de la tramitación de la ERSTIC (identificado o identificable)".

En este sentido, y dado que se está procediendo al tratamiento de datos de carácter personal que supone la inclusión de dichos datos en un fichero, considerado por la propia norma (artículo 3.b.), como "conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso", el mismo se encontrará sometido a la Ley, siendo obligada su inscripción en el Registro General de Protección de Datos, conforme dispone el artículo 26.

Por tanto, la Empresa Registrada Suministradora (ERSTIC) será responsable de tantos ficheros como conjuntos estructurados de datos, adscritos a una determinada finalidad legítima, según el artículo 4.1 de la Ley, utilice. Así, procederá la inscripción de un solo fichero o varios en función de la finalidad a la que se destinen los datos que se incluyen en el propio fichero.

En la actualidad, la notificación deberá verificarse mediante la presentación de los modelos normalizados contenidos en la Resolución de esta Agencia de 30 de mayo de 2000 (BOE de 27 de junio) por la que se aprueban los modelos normalizados en soporte papel, magnético y telemático. Los citados modelos se pueden obtener a través de Internet en la dirección: www.agpd.es.

Dicho esto, respecto al consentimiento que deben prestar los interesados al tratamiento de sus datos de carácter personal, debe señalarse que, si bien el artículo 6.1 de la Ley Orgánica 15/1999, dispone que, "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.", el apartado 2º del propio artículo indica que dicho consentimiento no será preciso cuando los datos de carácter personal se refieran a las partes de un contrato o precontrato de una relación laboral y sean necesarios para su mantenimiento o cumplimiento. Por tanto, en la medida en que los datos objeto del tratamiento sean únicamente los necesarios para el correcto desenvolvimiento de la relación comercial entre clientes y los datos sean necesarios para su mantenimiento y cumplimiento, no será necesario recabar el consentimiento del afectado. En caso contrario, será necesario requerir el consentimiento del



interesado que deberá ser, conforme a lo dispuesto en el artículo 3 h), "libre, inequívoco, específico e informado", debiendo en consecuencia aparecer vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos, siendo así que los datos únicamente podrían ser tratados en el ámbito de las mencionadas finalidades, tal y como dispone el citado artículo 4.1 de la Ley Orgánica, no pudiendo ser tratados para fines incompatibles con aquéllas (artículo 4.2 de la Ley Orgánica).

La manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realiza en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información.

El consentimiento, salvo cuando el tratamiento se refiera a los datos especialmente protegidos, regulados por el artículo 7 de la Ley Orgánica, podrá obtenerse de forma expresa o tácita, es decir, tanto como consecuencia de una afirmación específica del afectado en ese sentido, como mediante la falta de una manifestación contraria al tratamiento.

En todo caso, y aún en los supuestos de excepción a la prestación del consentimiento del interesado para el tratamiento de sus datos de carácter personal previstos en el artículo 6.2, la Ley impone el deber de información al afectado, al disponer su artículo 5.1 que "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

En consecuencia, el responsable del tratamiento deberá dar cumplida cuenta a lo dispuesto en el citado artículo 5, dado que aún en los supuestos en que no sea preciso el consentimiento del interesado, si deberá advertirse al mismo de los extremos contenidos en ese precepto.



Siguiendo con el contenido del capítulo 4º cuando refleja que la Empresa Registrada Suministradora "deberá informar a sus clientes de su derecho a acceder o disponer a la información recogida.....", se señala que el deber de información del responsable del fichero habrá de hacerse extensivo a lo señalado anteriormente, ofreciendo la posibilidad de ejercicio de los derechos de acceso, rectificación, cancelación y oposición previstos por la Ley, así como ante quién podrán efectuarse (artículo 5.1.d) y e)).

Por otro lado, lo reflejado en los apartados 4.6 y 4.7, relativos al mantenimiento de los datos en el registro y al control de seguridad y confidencialidad de los accesos, debe ponerse en conexión con lo dispuesto en la previsión general contemplada en el artículo 9 de la Ley 15/1999 sobre las medidas de seguridad que deberán adoptarse en cualquier tratamiento de datos de carácter personal, a tenor de cuyo apartado primero "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

De acuerdo con el apartado segundo de dicho artículo "No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas".

Así, por parte de la empresa responsable del fichero se deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, todo ello de acuerdo con las disposiciones contenidas en el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal, aprobado por el Real Decreto 994/1999 de 11 de junio.

II

En el capítulo 5º referido a los perfiles profesionales de las personas, nos indica que se recoge información profesional y laboral del personal de la Empresa Registrada Suministradora que será puesta a disposición de sus clientes.



A los efectos, tal y como señalábamos en el punto anterior en lo referente al tratamiento de los datos de los trabajadores que se ponen a disposición de los clientes deberá tenerse en cuenta la previsión del artículo 6.1 de la Ley respecto al consentimiento que deben prestar los interesados.

En lo referente al tratamiento de los datos correspondientes a los trabajadores, considerando que el mismo se efectúa en el ámbito de la relación laboral y la previsible finalidad de ese tratamiento, a la que posteriormente se hará referencia, debe señalarse que el artículo 6.2 de la Ley Orgánica 15/1999 exceptúa la obligación de recabar el consentimiento de los afectados en los supuestos en que "los datos de carácter personal ... se refieran a las partes de un contrato o precontrato de una relación....., laboral y sean necesarios para su mantenimiento o cumplimiento".

Por tanto, bastará con cumplir el deber de información contenido en el artículo 5.1 de la Ley (al que ya hacíamos referencia en el punto anterior), informando el empresario a los trabajadores del efectivo tratamiento de los datos, la finalidad y usos de los mismos, sus destinatarios y la posibilidad de ejercitar los derechos que la Ley Orgánica les concede (información que deberá efectuarse, como exige dicho artículo 5, de manera expresa, precisa e inequívoca).

Por otro lado, al tratarse de un registro que va a ser consultado por las empresas clientes y estará disponible para las auditorias y controles previstos en la Marca, no cabe duda que su difusión, aunque sea con acceso restringido, supondrá una cesión de datos de carácter personal que debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la Ley, donde se establece que la misma sólo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario y exige para que pueda tener lugar (salvo los supuestos exceptuados por el apartado segundo), el previo consentimiento del interesado, otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

En este sentido se consideran adecuadas las garantías previstas en los apartados "b.6" y "5.5" del capítulo que se comenta relativo a la autorización para asociar datos de identificación y a la obtención del consentimiento de sus empleados.



Y en todo caso, lo anterior debe ponerse en conexión con lo dispuesto por el artículo 4.3 de la Ley Orgánica 15/1999, que establece el denominado "principio de calidad de los datos", en virtud del cual "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado". Por este motivo, se impone que los datos de carácter personal incorporados a los ficheros de la consultante reflejen con exactitud y certeza la totalidad del contenido al que los mismos se refieren.

De ello se desprende que en el supuesto de que se produzcan variaciones en los datos contenidos en las bases de datos personales de la consultante debería procederse cuanto antes a su modificación o, en su caso, rectificación, a fin de reflejar la situación real de los afectados.

En cuanto a la conservación de los datos, resultará de aplicación el mandato del epígrafe 5 del artículo 4 de la Ley 15/1999 es decir, los datos de carácter personal deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que hubieran sido recabados o registrados. Añade además la Ley que los datos no serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines que determinaron su recogida o tratamiento.

Por otra parte, las disposiciones del capítulo 5º finalizan haciendo referencia al nombramiento de una persona encargada del control de seguridad y confidencialidad de los accesos. En este apartado de nuevo deberá observarse el principio de seguridad de los datos establecido en el ya citado artículo 9 de la Ley, que impone al responsable del fichero la necesidad de implantar las adecuadas medidas de seguridad que, sin perjuicio de lo establecido en el Real Decreto 994/1999, garanticen la adecuada integridad y confidencialidad de la información, habida cuenta de la finalidad que justifica el tratamiento de los datos en el presente supuesto,

III

En el capítulo 10, relativo a la contratación, deberá tenerse en cuenta que cuando la Empresa Registrada Suministradora sea contratada por una empresa cliente, y en la medida en que el servicio a prestar implique un acceso a datos de carácter personal responsabilidad de la empresa cliente se convertirá (la Empresa Registrada Suministradora), en lo que la Ley 15/1999 denomina encargado del tratamiento, es decir, según define el artículo 3 g) de la Ley "encargado del tratamiento: La persona física o jurídica, autoridad



pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.”

Dicho lo anterior, es necesario hacer constar que la relación jurídica entre la empresa cliente y la empresa encargada de prestar el servicio descrito es decir, la Empresa Registrada Suministradora, se ajuste a las obligaciones que la Ley impone, resumidas de la siguiente forma:

- En lo que atañe a los requisitos formales, el artículo 12.2 impone que “la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”.
- Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que “una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”.
- En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. La Agencia Española de Protección de Datos ha considerado que será posible la subcontratación de estos servicios siempre y cuando se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:
 - o a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.
 - o b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.
 - o c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.



- En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.
- Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen."

III

En el capítulo 12 relativo a la seguridad y confidencialidad de los datos de la empresa cliente, la Empresa Suministradora, tal y como señalábamos en el punto anterior, como encargada del tratamiento de los datos por cuenta de su responsable (la empresa cliente), deberá incorporar la medidas de índole técnica y organizativas que garanticen la seguridad y confidencialidad del tratamiento de los datos a los que accede y estas habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, esto es, las de nivel correspondiente a los datos incorporados al fichero, tal y como se desprende de lo previsto en los artículo 9 y 12.2 de la Ley Orgánica.

Conforme define el artículo 1 del Reglamento de Medidas de Seguridad, el mismo tiene por objeto establecer las medidas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de datos de carácter personal y por tanto, habrán de ser implantadas tanto por el responsable del fichero como por el encargado del tratamiento. Por su parte el artículo 4 establece los distintos niveles de seguridad tomando como punto de partida la información contenida en los distintos ficheros. Ello supone que cualquier operación de tratamiento realizada sobre un determinado fichero, una de las cuales sería la atribuida al encargado del tratamiento, deberá someterse a las medidas de seguridad que para ese fichero imponga el Reglamento.



IV

El capítulo 13 se refiere a las actualizaciones de software de los sistemas de información como un servicio que la Empresa Registrada Suministradora se compromete a ofrecer a las empresas clientes.

En estos supuestos, y en la medida en que la Empresa Registrada Suministradora como encargada del tratamiento ofrece el servicio añadido de actualización de software a sus clientes y para ello necesite a su vez subcontratar este tipo de servicios, desde la aplicación de la normativa sobre protección de datos de carácter personal, procede analizar la posibilidad de que un encargado del tratamiento subcontrate los servicios de un tercero.

Pues bien, en cuanto a la posibilidad de que el encargado del tratamiento pueda subcontratar los servicios de un segundo encargado, el artículo 12.2 de la Ley Orgánica 15/1999, al que hacíamos referencia en el **punto III**, y a cuyo contenido nos remitimos, establece que en las estipulaciones del contrato debería hacerse constar que el encargado del tratamiento no comunicará los datos, "ni siquiera para su conservación, a otras personas".

El fundamento de dicha previsión se deriva directamente de la propia naturaleza del derecho fundamental a la protección de datos de carácter personal. En este sentido, si dicho derecho consiste, según indica el Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, en un poder de disposición del afectado sobre la información que le concierne, resulta lógico que, habiendo autorizado (o habiendo previsto la Ley) que los datos puedan ser objeto de tratamiento por parte de un determinado responsable, será preciso que dicho responsable conozca en cada momento que terceras entidades acceden a dichos datos, siempre en su nombre, a fin de garantizar al interesado que los datos de los que el mismo es titular no excedan del control de aquella entidad cuyo tratamiento ha sido aceptado por aquél.

Si se estableciera la posibilidad de subcontratar sucesivamente dicho tratamiento sin conocimiento del responsable, éste carecería de conocimiento para poder atender cualquier reclamación efectuada por el afectado e incluso para conocer quién accede en cada momento a los datos de carácter personal cuyo tratamiento ha sido consentido por el interesado.

Teniendo en cuenta la consideraciones realizadas, sí sería posible la transmisión de los datos a un tercer subcontratista en caso de que el



responsable pudiera conocer específicamente esta circunstancia. Ello se lograría bien mediante su participación directa en el contrato con el tercero, bien encomendando un apoderamiento a tal efecto al encargado del tratamiento, bien haciéndose constar expresamente en el contrato firmado entre el responsable y el encargado la propia circunstancia de la subcontratación.

V

En el capítulo 14 se contemplan los compromisos que la Empresa Registrada Suministradora adquiere en los supuestos de rotación de los recursos humanos que se asignan a los proyectos contratados.

Así, en el apartado 14.2 se describen las obligaciones que asume la Empresa Registrada Suministradora ante posibles sustituciones de algunos de sus empleados en el proyectos.

En este sentido, el artículo 10 de la Ley 15/1999, impone tanto a los responsables del fichero como a aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal (es decir, responsable del fichero, encargado del tratamiento, personal de uno y de otro...), la obligación de guardar secreto profesional sobre los mismos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular o el responsable del fichero. Con ello queremos decir que sería aconsejable establecer una cláusula referida al deber de secreto por parte de los empleados del suministrador que resultan adscritos al proyecto del cliente y que por cualquier motivo tenga que ser sustituido.

VI

En el capítulo 15 se establecen las garantías que ofrece la Empresa Suministradora a la finalización de la prestación de los servicios a sus (empresas) clientes.

En este sentido, si como se indicó, la relación derivada del contrato de prestación de servicios sea la existente entre un responsable (la empresa cliente) y un encargado del tratamiento (la Empresa Registrada Suministradora), implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley Orgánica, de forma que "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier



soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”.

Cumplido este deber, el encargado no deberá conservar los datos relacionados con la prestación de servicios a menos que ello fuera necesario para atender a las responsabilidades derivadas de su contrato y para esta exclusiva finalidad.

El incumplimiento de esta previsión podría llevar aparejada la consecuencia, prevista en el artículo 12.4, al que ya nos hemos referido, de que “En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”.

En consecuencia sería conveniente incluir una estipulación referida al destino que habrá de darse a los datos, en el sentido previsto en el artículo 12.3 de la Ley Orgánica 15/1999.

Es cuanto tiene el honor de informar a V.I.

Madrid, 23 de marzo de 2007

**LA JEFE DE SERVICIO
DE LA UNIDAD DE APOYO A LA DIRECCIÓN**

Fdo.- Lourdes Hernández Crespo

Visto y conforme,
**EL ABOGADO DEL ESTADO
JEFE DEL GABINETE JURÍDICO**

Fdo. Agustín Puente Escobar

ILMO. SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS