

RINCON LEGAL

Régimen legal del acceso a los datos personales en las prestaciones de mantenimiento y soporte informático



El espinoso asunto de la protección de datos continua siendo una asignatura pendiente en el mundo de la informática, donde las enrevesadas subcontrataciones para la prestación de servicios -fundamentalmente de outsourcing y soporte de aplicaciones- cuando éstas conllevan un acceso a datos personales, se efectúan de forma poco transparente para el cliente y en contra de lo establecido en la normativa sobre protección de datos personales.

[Ana Marzo Portera. Marzo & Abogados]

Ningún cambio de criterio ha tenido nuestro legislador en esta materia desde que en el año 1999 fuera aprobada la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Así, la contratación de una prestación de servicios (aunque sean de carácter informático) por una empresa a otras terceras, cuando dicha prestación conlleva un acceso a datos personales, está sujeta a una serie de requerimientos legales que ni la empresa de servicios ni la empresa cliente pueden o deben soslayar, so pena de incurrir en una infracción administrativa de carácter grave.

Veamos a continuación algunas cuestiones al respecto. Para empezar, el contratista pasa a denominarse "encargado del tratamiento" o lo que es igual, persona física o jurídica, pública o privada, u órgano administrativo o ente sin personalidad jurídica que actúa en el tráfico como sujeto diferenciado que, solo o conjuntamente con otros, trata datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Dicha definición, contemplada en el RDLOPD, resulta interesante a efectos de poner de manifiesto que el prestador del servicio es un mero ejecutor de la voluntad de la empresa cliente o responsable del fichero o tratamiento en términos legales.



En segundo lugar, y en lo que respecta a los requisitos formales, el artículo 12 de la LOPD impone que la realización de tratamientos de datos por cuenta de terceros esté regulada por escrito o en alguna otra forma que permita acreditar su celebración y contenido. En este sentido, la jurisprudencia ha sido tajante al respecto al señalar que la validez de la oferta y la aceptación de los servicios entre las partes, así como los documentos mercantiles y civiles que éstas suscriban al respecto, no son válidos a la hora de valorar la suficiencia desde el punto de vista del cumplimiento de los requisitos sobre protección de datos de carácter personal.

Así, la necesaria protección de los derechos de los afectados y titulares de los datos que serán objeto de tratamiento por el prestador del servicio,

obliga a que se exija una documentación más rigurosa que la simplemente mercantil para la validez del contrato de acceso a datos en cuestión ya que el contrato de servicio, si bien puede ser suficiente a los efectos civiles ó mercantiles, no sea bastante para garantizar los derechos relativos a la protección de datos.

En tercer lugar, en el contrato de acceso a datos se establecerá expresamente que el prestador encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento y 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.

Subcontratación

En cuarto lugar, en lo referente a la posible subcontratación de los servicios prestados, el reglamento de desarrollo de la LOPD es contundente: permite esta posibilidad sólo en caso de que el responsable del fichero apodere al prestador del servicio o encargado para la celebración del segundo contrato en nombre de aquél o cuando se den los siguientes requisitos:

– Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. En caso en que dicha circunstancia no se hubiera previsto en el contrato y la subcontratación

fuera necesaria, las partes deberán proceder a la modificación posterior del contrato. A tales efectos, en caso de que en el contrato no conste la identificación de la empresa subcontratista será preciso que el prestador encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

– Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

– Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato previsto en el artículo 12 de la LOPD.

Al respecto, es preciso aclarar que en el sector de la informática raramente el prestador de servicios actúa de forma transparente en este punto, en particular en periodos en que por cuestiones de falta personal el contratista principal utiliza el recurso de la subcontratación sin advertir al cliente de este hecho o de las circunstancias en que se pacta dicha subcontratación con el tercer subcontratista. Esta forma de actuar, que quizás simplemente responde a un problema de imagen por parte del contratista principal, es evidentemente contraria a la LOPD cuya máxima en este punto es la total y absoluta transparencia.

Estos condicionantes son igualmente trasladables a las partes de una relación contractual, por ejemplo en los casos de prestación de soporte y mantenimiento informático, cuando la intención del contratista principal es externalizar en un tercer subcontratado parte del servicio contratado por el cliente, y dicho subcontratado se encuentra ubicado fuera de España.

En este punto además, según reiterada doctrina administrativa de la Agencia Española de Protección de Datos, si bien la subcontratación de los servicios por parte de un encargado del tratamiento resulta posible cuando el subcontratista se encuentra en



territorio español, dicha subcontratación no es, más, posible en caso de encontrarse el subcontratista en un tercer país que no ofrece un nivel adecuado de protección para la transferencia internacional de datos, siendo preciso que el responsable sea parte en la relación jurídica y debiendo, en todo caso, apostarse las adecuadas garantías encaminadas a la obtención de la preceptiva autorización del Director de la Agencia Española de Protección de Datos prevista en el artículo 33.1 de la LOPD.

Medidas de seguridad

En quinto lugar, y en relación con la prestación del servicio y las medidas de seguridad que hayan de ser adoptadas por las partes, además de la necesidad de determinar el nivel a establecer, la responsabilidad es compartida de la siguiente manera:

– Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsa-

ble, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

– Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

– Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 del reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

Por último, en lo que respecta a la finalización del servicio, la LOPD establece que, una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

A la vista de todo lo anterior, no podemos sino recomendar a cualquier entidad, pública o privada que vaya a contratar un servicio de mantenimiento o soporte informático con un tercero, que verifique el cumplimiento de los requisitos anteriores establecidos por la normativa vigente en protección de datos de carácter personal. □

Marzo & Abogados

DERECHO Y NUEVAS TECNOLOGÍAS

Suscríbete gratis

¡Suscríbete gratis a nuestra revista AUSAPE!

La revista AUSAPE es el medio de comunicación directo de esta Asociación con sus empresas asociadas. En ella se informa de todas las actividades llevadas a cabo por AUSAPE, además de incluir información de primera mano sobre las últimas novedades tecnológicas que afectan al sector de las TIC.

Si todavía no estás suscrito y quieres recibir esta revista, totalmente gratis, rellena el siguiente cupón y envíalo por fax al número: **91 519 52 85**. También puedes mandarnos un e-mail a secretaria@ausape.es incluyendo en él los datos que se solicitan.

Empresa:

Asociado de AUSAPE (SÍ NO):

Nombre:

Cargo:

Dirección:

CP:

Población:

Provincia:

Teléfono:

E-mail:

Asociación de Usuarios de SAP España
Emilio Vargas, 1 - 1 Izd. (Edif. FITENI II)
28043 Madrid
Teléfono: 91 519 50 94 / Fax: 91 519 52 85
e-mail: secretaria@ausape.es
Web: www.ausape.es