Informe 0245/2010

La consulta plantea si la fusión entre las diversas empresas que componen el grupo consultante, en el que cada compañía mantiene su personalidad jurídica propia, permite que sólo se deban notificar un solo fichero de datos a esta Agencia, así como la elaboración de un documento de seguridad y realización de auditorías de seguridad únicos para todas ellas, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

I

Del contenido de la consulta, no se desprende claramente si se prevé la creación de una base de datos centralizada, que se sustentaría de los datos de los empleados que envíen a la misma las distintas empresas que forman el grupo, o si alguna de las empresas va a realizar alguna prestación de servicios para las demás en relación con el tratamiento de los datos que pudiera encajarse en la figura del encargo de tratamiento del artículo 12 de la LOPD, ni se concretan los tratamientos, usos o cesiones de datos que pretenden hacer de dichos datos, se procede a dar una respuesta general.

En primer lugar conviene señalar que es criterio uniforme de la Agencia Española de Protección de Datos, que la existencia de un grupo de empresas no afecta para que cada una de las sociedades integradas en el mismo no mantenga diferenciada y plena su personalidad jurídica. A todos los efectos jurídicos, la circunstancia de que una sociedad esté participada por otra, no afecta al hecho de que ambas sean distintas personas, de modo que la comunicación de datos se produce entre dos personas distintas, sin que exista una previsión legal que flexibilice los requisitos para la legitimidad de dicha cesión.

Este criterio ha sido ratificado por la Sentencia de la Sección Novena de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid, de 16 de octubre de 2000, cuando en su fundamento de derecho cuarto señala que, “Cualquier empresa es libre de constituirse en cualquiera de las formas societarias que el Derecho Mercantil regula. Asimismo, las empresas pueden unirse a través de las distintas formas reguladas en derecho: fusión, Absorción, etc. Pero, desde luego, lo que no cabe es que existan dos sociedades anónimas y, como tales, independientes y con personalidad jurídica autónoma y que por el hecho de que una sea propiedad de la otra, el particular que contrata con la primera pueda verse perjudicado, precisamente, por la estructura empresarial que la sociedad ha elegido. Si la recurrente ha preferido constituir dos sociedades y trabajar con ellas de manera independiente, beneficiándose así del mantenimiento de dos personas jurídicas distintas, no

puede, al mismo tiempo, pretender justificar el conocimiento por parte de la matriz de los datos que le constan a la filial por las operaciones que esta última ha intervenido pues ello supone olvidarse de que se trata de personas jurídicas distintas".

Atendiendo a lo que acabamos de indicar, cada una de las empresas que integran el grupo será responsable del fichero de datos de sus correspondientes empleados, teniendo en cuenta que el artículo 3 d) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal define al mismo como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento." Es decir, que cada empresa del grupo gestionaría sus datos.

En consecuencia si por parte de alguna de las empresas pertenecientes al grupo, se produce un acceso a los datos de cualquiera de las otras que componen dicho grupo, o se produce el acceso a dicha información mediante la creación de una base de datos común, nos encontraríamos ante una situación clara de comunicación o cesión de datos entre empresas, definida en el artículo 3 i) de la Ley Orgánica 15/1999, como "Toda revelación de datos realizada a persona distinta del interesado" y esta cesión requerirá el consentimiento del afectado conforme establece el artículo 11.1 de la Ley Orgánica 15/1999, al disponer que: "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".

El consentimiento del interesado sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2, cuyo apartado c) prevé expresamente la posibilidad de proceder a la cesión inconsentida "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".

A nuestro juicio, de acuerdo con lo dispuesto en dicho precepto, la conexión con ficheros de terceros al que se refiere el presente informe, no encontraría encaje en lo dispuesto en el transcrito artículo 11.2 de la Ley Orgánica.

En definitiva, la incorporación de los datos de los empleados a una base de datos centralizada o común, exige que cada empresa haya informado debidamente a los afectados en los términos del artículo 5.1 de la Ley Orgánica 15/1999 y que haya obtenido el consentimiento de éstos para la incorporación de su información personal en dicha base de datos.

Cualquier acceso a los datos entre las diferentes sociedades que componen el grupo constituye un supuesto de cesión que requiere el consentimiento del afectado o la habilitación legal para la misma.

En consecuencia, resulta aplicable al supuesto objeto de consulta la regla general del artículo 11.1 de la Ley Orgánica, anteriormente transcrito, a menos que medie el consentimiento del afectado al que se refiere dicho precepto legal. En este sentido, siempre que se proceda al tratamiento de datos personales, definidos por la Ley (artículo 3.a).), como "cualquier información concerniente a personas físicas identificadas o identificables", que suponga 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 fichero se encontrará sometido a la Ley, siendo obligada su inscripción en el Registro General de Protección de Datos. Por tanto, cada sociedad será responsable de forma individual, de tantos ficheros como conjuntos estructurados de datos, adscritos a una determinada finalidad legítima, según el artículo 4.1 de la Ley, utilice.

De manera que el supuesto de fusión consultado, en el que cada sociedad del grupo mantiene su personalidad jurídica diferenciada, no produce la modificación del responsable de los ficheros.

Atendiendo a lo que acabamos de indicar, cada una de las empresas del grupo deberá proceder a notificar de manera independiente sus propios ficheros, tal y como exigen los artículos 26 y 39 de la Ley Orgánica 15/1999, de 13 de diciembre, notificación que podrá realizarse por vía telemática, a través del sistema NOTA que figura en la página web de este Organismo. Cada una de las empresas que han formado el grupo asumirá la titularidad de los ficheros que son de su responsabilidad, sin que pueda hablarse de un fichero del grupo.

II

Sentado lo anterior, la cuestión relativa a si sería posible la adopción de un documento de seguridad único para las diferentes empresas ha de resolverse teniendo presente que el artículo 9 de la LOPD atribuye a cada responsable del fichero el cumplimiento de las medidas de seguridad en los términos que se describen en los artículos 79 y siguientes del Reglamento.

El artículo 88 del Real Decreto 1720/2007 establece que "1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente, que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o

tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización."

La conclusión a la cuestión planteada ha de ser la de que siendo cada empresa responsable de los ficheros propios de su sistema de información, el documento de seguridad (ya sea individual o varios agrupados) deberá ser específico de cada empresa del grupo, comprendiendo el contenido mínimo señalado en el número 3 del artículo 88. Además, al ser un documento interno de la organización del responsable, deberá identificar a éste indubitadamente y en cuanto debe dar a conocerse a los trabajadores (apartado c)) las funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros, deberá ir refrendado por el máximo responsable en la organización de la empresa.

En cuanto a la obligación de realizar una auditoría, teniendo en cuenta que la misma tiene por finalidad verificar cada dos años el cumplimiento de las medidas de seguridad, identificar las deficiencias de los sistemas de información e instalaciones y proponer las medidas correctoras al responsable de seguridad competente de cada empresa, que, a su vez, las elevará al responsable del fichero (artículo 96 del Reglamento), y además, que es un documento propio de la organización de cada empresa, dicha auditoría deberá realizarse por cada responsable de los ficheros, es decir, por cada empresa del grupo.