



PERÚ

Ministerio de Justicia y Derechos Humanos

Despacho Viceministerial de Derechos Humanos

Dirección General de Protección de Datos Personales

CARGO

"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

Miraflores, 23 ABR 2015

Oficio N° 213 -2015-JUS/DGPDP

Señora:

ESTUDIO DALY, OTERO, FLOREZ & NUÑEZ DEL PRADO.  
Calle Río De La Plata N° 167. Oficina N° 201. San Isidro. Lima.  
Presente.-

Referencia : a) Documento con registro N° 017160 de 20 de marzo de 2015.  
b) Oficio N° 405-2015-JUS-DGPDP-DRN de 30 de marzo de 2015.

Me dirijo a usted con relación al asunto de la referencia con la finalidad de absolver su consulta.

Como marco general, es oportuno mencionar que la Autoridad Nacional de Protección de Datos Personales, en adelante la **APDP**, conforme con lo establecido por el numeral 10 del artículo 33 de la Ley N° 29733, Ley de Protección de Datos Personales, en adelante la **LPDP**, tiene la facultad para absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.

En consecuencia, no absolvemos consultas sobre casos concretos o particulares que constituyan asesoría jurídica, sino sobre la interpretación de alguna disposición contenida en la LPDP y su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS.

En ese orden de ideas, atendemos la consulta formulada en los siguientes términos:

**Marco legal:**

1. La Constitución Política del Perú dispone, en el numeral 6 del artículo 2, que toda persona tiene derecho "(...) a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (...)".

En desarrollo del mencionado derecho constitucional se publicó el 3 de julio de 2011, la LPDP, que establece en su artículo 1 que tiene como objeto "(...) garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen (...)".

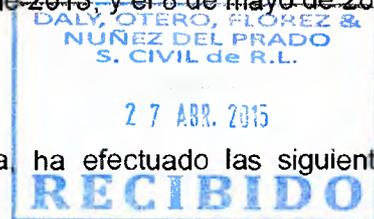
El Reglamento de la LPDP, se aprobó el 22 de marzo de 2013, y el 8 de mayo de 2013 entró en plena vigencia conjuntamente con la LPDP.

**Objeto de la consulta:**

2. La solicitante con documento a) de la referencia, ha efectuado las siguientes consultas:



J. A. Quiroga L.





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Despacho  
Viceministerial de  
Derechos Humanos

Dirección General  
de Protección de  
Datos Personales

*"(...) En el formulario de registro, en el punto II.4 se solicita la ubicación física del banco de datos personales. ¿Qué ocurre en los casos en los que los bancos de datos se almacenan en la nube (...)"*

*"(...) ¿De qué manera se podría completar el punto IV medidas de seguridad, cuando todo el manejo de los datos personales (almacenamiento, procesamiento, custodia, etc) está tercerizado con otra compañía a través de un contrato? (...)".*

3. En cuanto a la **primera consulta**, el artículo 33 del Reglamento de la LPDP regula el tratamiento de datos personales por medios tecnológicos tercerizados, el cual es aplicable cuando el tratamiento se terceriza de acuerdo a los servicios que se conocen como computación en la nube o "cloud computing".

El servicio permite a quien lo contrata gestionar la información de forma virtual, por lo que el tratamiento de datos personales se da mediante el empleo de internet, utilizando recursos de hardware, software, almacenamiento, servicios y comunicaciones que se encuentran distribuidos geográficamente y a los que se accede a través de redes públicas.

Por ello, en líneas generales, la computación en la nube o "cloud computing", puede clasificarse en:

(i) Pública, cuando quien requiere el servicio de computación en la nube o "cloud computing" tiene una relación contractual con el prestador del servicio, quien a su vez, le proporcionará los recursos necesarios para gestionar y administrar su información en la nube.

(ii) Privada, cuando la propia entidad controla, gestiona y administra sus servicios mediante computación en la nube o "cloud computing" para los conglomerados que la conforman, sin que en la misma participen entidades externas. En este caso, puede contratarse un tercero que actuará bajo la supervisión de la entidad y en función de sus necesidades.

En ambos supuestos, conforme con lo establecido por el artículo 33 del Reglamento de la LPDP, el tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, sea nube pública o privada, podrá ser contratado por el responsable del tratamiento de datos personales siempre y cuando para la ejecución de aquel se garantice el cumplimiento de lo establecido por la LPDP y su Reglamento.

En consecuencia, el titular del banco de datos personales o responsable del tratamiento, que contrata servicios de computación en la nube o "cloud computing", continúa siendo responsable del tratamiento.

Quien ofrece el servicio de computación en la nube o "cloud computing" es un prestador de servicios quien, dentro del marco normativo de la LPDP y su Reglamento debe proporcionar ciertas condiciones o mecanismos al responsable del tratamiento.

Por ellos, no representa ninguna dificultad que el responsable del tratamiento (quien contrata el servicio de computación en la nube o "cloud computing") obtenga la información requerida en el formulario.



J. A. Quiroga L.



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Despacho  
Viceministerial de  
Derechos Humanos

Dirección General  
de Protección de  
Datos Personales

Por lo expuesto, corresponde al responsable del tratamiento verificar que al contratar el servicio de computación en la nube o "cloud computing" se le brinde información clara, precisa y completa sobre dónde, cuándo y quién ha procesado los datos personales (dentro de los recursos que le ofrece el prestador del servicio o de la cadena de subcontrataciones en la cual se apoya), puesto que dicha circunstancia tiene evidente relevancia.

Adicionalmente, el numeral 5 del artículo 77 del Reglamento de la LPDP establece que será objeto de inscripción en el RNPDP las comunicaciones referidas al flujo transfronterizo de datos personales.

En resumen, el responsable del tratamiento deberá obtener la información de ubicación de su proveedor de servicios, pues lo contrario sería admitir que hace tratamientos pero desconoce donde ocurre una parte de ellos, que puede ser la más importante.

4. En cuanto a la **segunda consulta**, resulta de aplicación lo establecido por el numeral 3 del artículo 35 del Reglamento de la LPDP, que regula los mecanismos para la prestación del servicio de tratamiento de datos personales por medios tecnológicos tercerizados, y determina que la prestación del servicio debe hacerse garantizando medidas de seguridad adecuadas para la protección de los datos personales sobre los que presta el servicio, de acuerdo a lo previsto en los artículos 34 y 35 del Reglamento de la LPDP.

En resumen, el responsable del tratamiento deberá proveer contractualmente los niveles de seguridad adecuados por parte del prestador del servicio.

5. Finalmente, con documento **b)** indicado en la referencia, la DRN ha puesto en conocimiento de la APDP el siguiente criterio adoptado para un mejor llenado del formulario de inscripción:

*"(...) Esta Dirección considera que si la información de seguridad no se adapta a las preguntas que figuran en el punto IV del formulario de inscripción, el titular del banco podrá adjuntar una hoja adicional indicando las medidas de seguridad implementadas por el prestador del servicio y la forma en que, como cliente, comprueba su cumplimiento. Toda vez que, de acuerdo al artículo 79 del Reglamento de la LPDP para inscribir un banco de datos personales es necesario informar la descripción técnica de las medidas de seguridad (...)"*

Atentamente,

JOSÉ ALVARO QUIROGA LEÓN  
Director General de Protección de Datos Personales  
Ministerio de Justicia y Derechos Humanos





PERU

Ministerio  
de Justicia  
y Derechos Humanos

Despacho  
Viceministerial de  
Derechos Humanos

Dirección General de Protección  
de Datos Personales

## II. CONSULTA

Acorde con el artículo 33º del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales nos da la facultad de tercerizar los medios de almacenamiento y procesamiento de nuestros bancos de datos personales; sin embargo, en el formulario de registro, en el punto "II.4" solicita la "UBICACIÓN FÍSICA DEL BANCO DE DATOS PERSONALES", ¿qué ocurre en los casos en los que los Bancos de Datos se almacenan en la "nube" ?

(En inglés se le llama Cloud computing. O tan solo The cloud. Es un modelo de uso de las computadoras. Lo que normalmente estaría en una PC o un disco duro (por ejemplo programas o archivos) pasa a estar almacenado en un conjunto de servidores a los que puedes acceder a través de Internet y que forman la tal nube. Dichos servidores pueden estar ubicados en varios lugares, sin que toda la información este almacenada en un punto geográfico específico o determinado).

El concepto de "nube" no está ligado a una ubicación física determinada ya que por las características propias de esta modalidad de almacenamiento de información, los servidores donde se almacena la información pueden estar dispersos por todo el mundo. Por esta razón solicitamos la precisión para el correcto llenado todo este punto en base al caso antes señalado.

Asimismo, ¿de qué manera se podría completar el punto IV MEDIDAS DE SEGURIDAD, cuando todo el manejo de los datos personales (almacenamiento, procesamiento, custodia, etc.) está tercerizado con otra compañía a través de un contrato?

Ponemos el siguiente ejemplo para poder ser lo más específicos posibles:

La empresa "A", domiciliada en el Perú, ofrece a través de su página web una serie de productos y servicios, previo registro de sus clientes para que estos sean contactados para los fines estrictamente comerciales.

La empresa "B" es una empresa domiciliada en los Estados Unidos y ofrece el servicio de almacenamiento en la "Nube", procesamiento, custodia y envió de correos promocionales, por lo que es esta empresa la que posee los manuales de seguridad y todos los mecanismos para asegurar el cumplimiento de la normativa de protección de datos personales que es contratada por la empresa "A". La empresa "A" no recibe ni maneja en ningún momento los datos personales todo se terceriza, el único contacto que tiene la empresa "A" con sus usuarios es ante el planteamiento de un reclamo por los servicios ofrecidos porque el usuario escribe directamente un correo de reclamo a la empresa "A" quien debe subsanar el mismo.

En el mismo ejemplo antes citado ¿A quién se nombraría como persona responsable? Ya que en estos casos no es posible señalar a un empleado o persona natural de la empresa "B" ya que todos sus sistemas están automatizados y ante caso de alguna falla técnica, las comunicaciones no se realizan dirigidas a una persona en específico sino al área de soporte técnico.

En virtud de lo señalado, **SOLICITO** la absolución de consulta a la Dirección General de Protección de Datos Personales, conforme al numeral 10 del artículo 33º de la Ley N° 29733- Ley de Protección de Datos Personales.

Fecha:

20/03/2015

Firma:

