INTERBEL S)

2013

Riesgos legales de contratar Gmail u Office 365

Interbel S)

www.interbel.es

902 39 39 39

Con el asesoramiento jurídico de

Derecho.com

Resumen de los riesgos para las empresas que usan Office 365 o Gmail

Este documento ha sido elaborado con la intención de informar de los riesgos que puede sufrir una empresa española al utilizar los servicios de correo electrónico ofrecidos por empresas de Estados Unidos, que podemos resumir en:

1) **Obligatoria notificación de la transmisión internacional de datos a la AEPD:**

   LOPD: Las empresas que trabajan con Gmail u Office 365 deben llevar a cabo un trámite adicional que consiste en notificar la transferencia internacional de datos a la Agencia Española de Protección de Datos, para cumplir con la LOPD. La multa para las empresas que no realizan el trámite puede llegar a ser de **hasta 40.000€**

2) **El sometimiento de los servicios de correo electrónico a la USA Patriot Act podría provocar que empresas españolas llegasen a incumplir la LOPD.**

   LOPD: los clientes podrían llegar a demandar ante la AEPD a las empresas que utilizan estos proveedores por incumplimiento de la LOPD debido a la vulnerabilidad de la privacidad por el riesgo de que sus datos personales puedan ser vistos por terceros. El coste para las empresas puede llegar a ser de **hasta 300.000€.**

3) **Pérdida de confidencialidad con empresas colaboradoras y clientes**

   CONFIDENCIALIDAD: cuando las empresas tienen firmado un contrato de confidencialidad con un cliente, éste le puede demandar al utilizar un servicio de Gmail u Office 365 ya que no tiene garantizada la confidencialidad pactada.

4) **Pérdida de competitividad**

   ESPIONAJE INDUSTRIAL: los correos internos con datos relevantes del negocio pueden ser vistos en cualquier momento y la información contenida en dichos emails puede acabar en manos de sus competidores estadounidenses.

¿Cuáles son los riesgos para las empresas que usan Gmail u Office 365?

1. Obligatoria notificación de la transmisión internacional de datos a la AEPD

Los datos almacenados en los servidores de Gmail o Microsoft Office 365 pueden estar en cualquier país, incluyendo los EEUU, sin tener en cuenta la nacionalidad del titular de los datos ni estar sometidos a otra legislación que la norteamericana en lo concerniente a privacidad y confidencialidad.

Cuando las empresas contratan el servicio de correo electrónico a un proveedor localizado en EE.UU. siempre se considera transferencia internacional de datos.

LOPD: Las empresas que trabajan con Gmail u Office 365 deben llevar a cabo un trámite adicional que consiste en notificar la transferencia internacional de datos a la Agencia Española de Protección de Datos, para cumplir con la LOPD. La multa para las empresas que no realizan el trámite puede llegar a ser de hasta 40.000€

2. El sometimiento de los servicios de correo electrónico a la USA Patriot Act podría provocar que empresas españolas llegasen a incumplir la LOPD.

El gobierno de EEUU, bajo el paraguas 'Patriot Act', puede aplicar todas y cada una de sus leyes a estos datos sin tener en cuenta el acuerdo Safe Harbor de protección de datos acordado entre los EE.UU y la UE[1]. Esto significa que el gobierno de EEUU puede acceder a la información de Gmail u Office 365 sin notificarlo y entrando en conflicto con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (en adelante, "**LOPD**")[2].

Este ha sido un duro golpe a la confianza respecto a la seguridad de sus datos entre los clientes y las empresas que usan estos proveedores de servicios de email.

LOPD: los clientes podrían llegar a demandar ante la AEPD a las empresas que utilizan estos proveedores por incumplimiento de la LOPD debido a la vulnerabilidad de la privacidad por el riesgo de que sus datos personales puedan ser vistos por terceros. El coste para las empresas puede llegar a ser de hasta 300.000€.

[1] Texto completo: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

[2] Texto completo: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

La sanción que se aplica depende del nivel de seguridad exigible en función el tipo de información que contienen los correos electrónicos:

NIVEL SEGURIDAD EXIGIBLE	OBLIGADOS	TIPO DE INFORMACIÓN
ALTO	Clínicas, hospitales, consultas médicas, laboratorios, sindicatos, partidos políticos, abogados y procuradores, prisiones y comisarias.	Informes médicos, datos de salud, información de accidentes, datos sobre infracciones administrativas o penales, datos de afiliación sindical.
MEDIO	Administraciones tributarias, entidades financieras, entidades gestoras, aseguradoras, mutuas de trabajo y accidentes, empresas de gestión de cobro, empresas de selección de personal.	Datos económicos y financieros, información sobre la solvencia patrimonial y crédito o cobro deudas, datos derivados de procesos de selección de personal.
BAJO	Cualquier empresa u organismo público que trate datos personales.	Cualquier tipo de dato personal.

3. **El sometimiento de los servicios de correo electrónico a la USA Patriot Act podría provocar el incumplimiento de los compromisos de confidencialidad.**

CONFIDENCIALIDAD: cuando las empresas tienen firmado un contrato de confidencialidad con un cliente, éste le puede demandar al utilizar un servicio de Gmail u Office 365 ya que no tiene garantizada la confidencialidad pactada.

Por ejemplo:

EMPRESAS	TIPO DE INFORMACIÓN
Agencias de Publicidad, Consultoras, proveedores de componentes de I+D de las empresas.	Anuncios, campañas, estrategias de marketing, planes de negocio, desarrollo de productos, resultados de investigación.

4. **Pérdida de competitividad**

ESPIONAJE INDUSTRIAL: los correos internos con datos relevantes del negocio pueden ser vistos en cualquier momento y sin previo aviso, lo que genera una falta de seguridad en las empresas de que la información contenida en sus emails no se transfiere a sus competidores estadounidenses.

A continuación se detallan los ASPECTOS JURÍDICOS a tener en cuenta al contratar una empresa de servicios de correo electrónico, un informe elaborado por Derecho.com en colaboración con Interbel.

¿QUÉ DEBE TENER EN CUENTA UNA EMPRESA ESPAÑOLA AL CONTRATAR UN SERVICIO DE CORREO ELECTRÓNICO TIPO GMAIL U OFFICE 365?

Es principalmente en materia de protección de datos personales donde la contratación de un servicio de correo electrónico (más aún si es en modalidad *cloud computing* o en la nube) exige tomar determinadas cautelas.

Así, no cabe duda de que el correo electrónico de una empresa contiene multitud de datos personales, por lo que su proveedor de servicios de correo electrónico se convierte en lo que jurídicamente se conoce como **encargado del tratamiento**[3] y el servicio de correo electrónico en un **tratamiento de datos**[4]**,** ambos plenamente sometidos al cumplimiento de la normativa española de protección de datos personales, esto es, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "**LOPD**") y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, "**RLOPD**").

De este modo, la empresa que se disponga a contratar dicho servicio deberá tener en cuenta lo siguiente:

a) **OBLIGACIONES CONTRACTUALES**
b) **LOCALIZACIÓN DEL PROVEEDOR**

[3] Art. 5.1.i) RLOPD: "*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 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. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.*"

[4] Art. 5.1.t) RLOPD: "*Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*"

a) **OBLIGACIONES CONTRACTUALES:**

Según establecen los artículos 12 de la LOPD y 20, 21 y 22 del RLOPD, antes de que el servicio de correo electrónico empiece a prestarse es preciso que la empresa cliente y el proveedor formalicen un contrato en el que, como mínimo, deberán hacerse constar los siguientes aspectos:

- Que el proveedor únicamente tratará los datos conforme a las instrucciones de la empresa cliente, 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.
- Las medidas de seguridad a que se refiere el artículo 9 de la LOPD y que el proveedor está obligado a implementar (nivel básico, medio o alto).
- Que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a la empresa cliente, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. En este sentido, conviene regular detalladamente la portabilidad de los datos.
- Que el proveedor no podrá subcontratar la prestación del servicio. Si fuera necesaria alguna subcontratación, esta deberá preverse en el contrato identificando, si es posible, a la empresa que la llevará a cabo. Cuando no se pueda identificar a la empresa subcontratista, se especificará la parte del servicio que podrá ser subcontratada y, en todo caso, antes de que la subcontratación se llegue a producir, el proveedor deberá comunicar a la empresa cliente la identidad del subcontratista.
- Que el proveedor y los posibles subcontratistas deberán formalizar un contrato en los mismos términos que el formalizado entre la empresa cliente y el proveedor.

Si bien es cierto que dicho contrato puede llegar a formalizarse mediante la adhesión por parte de la empresa cliente a unas condiciones generales creadas por el proveedor en el marco de un proceso de contratación online, es frecuente que dichas condiciones generales **no contengan todos los aspectos antes indicados, siendo además normalmente muy difícil poder formalizar con dichos proveedores otra documentación que subsane las carencias detectadas**.

- Empezar a utilizar un servicio de correo electrónico sin haber formalizado el contrato antes indicado, constituye una infracción tipificada como leve en el artículo 44.2.d) de la LOPD, **sancionable con multa de 900 a 40.000 euros.**

b) LOCALIZACIÓN DEL PROVEEDOR:

No sólo hay que conocer exactamente la localización física de la sede del proveedor del servicio de correo electrónico con el que vamos a contratar, sino también la de los distintos recursos físicos que integrarán el servicio, esto es, dónde van a estar realmente almacenados los datos o dónde van a ser tratados. La importancia de conocer dicha información radica en mantener en todo momento el control de los datos de la empresa y en la posibilidad de que se produzca una **transferencia internacional de datos**[5].

Así, dependiendo de la localización del proveedor del servicio de correo electrónico podemos encontrarnos en los siguientes escenarios:

a) **Proveedores localizados dentro del Espacio Económico Europeo (Países de la Unión Europea e Islandia, Liechtenstein y Noruega):** Todos los países pertenecientes al Espacio Económico Europeo están bajo el paraguas de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "**Directiva 95/46/CE**"), por lo que se considera que ofrecen un nivel adecuado de protección de datos. La contratación del servicio de correo electrónico a un proveedor localizado en el Espacio Económico Europeo no se considera transferencia internacional de datos y, por lo tanto, no requiere de trámites adicionales al respecto.

b) **Proveedores localizados en Hungría; Suiza; Nueva Zelanda; Canadá; Argentina; Uruguay; Guernsey; Isla de Man; Islas Feroe; Israel; Jersey y Andorra:** La Comisión Europea ha reconocido a dichos países un nivel adecuado de protección de datos. La contratación del servicio de correo electrónico a un proveedor localizado en cualquiera de estos países siempre se considera transferencia internacional de datos, si bien el único trámite adicional que se requiere es notificar la transferencia internacional a la Agencia Española de Protección de Datos, pero sólo a efectos informativos.

c) **Proveedores localizados en EE.UU:** EE.UU. como país no tiene actualmente reconocido por la Comisión Europea un nivel adecuado de protección de datos. No obstante, mediante la Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE, se establece que las empresas estadounidenses que se adhieran a los principios de **Safe Harbor** (Puerto Seguro) sí tendrán reconocido un nivel de protección de datos adecuado. Por tanto, antes de contratar el servicio de correo electrónico a un proveedor localizado en EE.UU., conviene verificar si se encuentra adherido o no a los principios de Safe Harbor (https://safeharbor.export.gov/list.aspx).

[5] Art. 5.1.s) RLOPD: *"Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."*

La contratación del servicio de correo electrónico a un proveedor localizado en EE.UU. siempre se considera transferencia internacional de datos. No obstante, se pueden dar dos situaciones distintas:

1ª: El proveedor está adherido a Safe Harbor: En ese caso, el único trámite adicional que se requiere es notificar la transferencia internacional a la Agencia Española de Protección de Datos, pero sólo a efectos informativos. Éste trámite debe realizarlo la empresa española que contrata estos servicios de correo electrónico.

> A modo de ejemplo, Microsoft Corporation (sita en Redmond, Washington) y las filiales estadounidenses controladas por ella están adheridas a Safe Harbor. También lo están Google Inc. (sita en Mountain View, California) y algunas de las filiales estadounidenses controladas por ella.

2ª: El proveedor no está adherido a Safe Harbor: En ese caso se requiere que el Director de la Agencia Española de Protección de Datos autorice la transferencia internacional de datos, para lo cual la empresa cliente le debe presentar:

1.- Solicitud formal de la autorización.

2.- Copia de las Cláusulas tipo 2010/87/UE (contenidas en la Decisión de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE) firmadas por la empresa cliente y el proveedor, en idioma español. Si el original no se ha firmado en este idioma, deberá presentarse una traducción jurada.

3.- Poder suficiente de todos los firmantes de las Cláusulas tipo 2010/87/UE.

Si el proceso de solicitud de autorización transcurre sin problemas, su concesión puede tardar en producirse hasta tres meses, no pudiendo utilizarse el servicio de correo electrónico hasta obtener la autorización.

En la práctica, **puede resultar harto difícil que determinados proveedores localizados en EE.UU. se avengan a facilitar la documentación requerida para solicitar la autorización al Director de la Agencia Española de Protección de Datos.**

> En el caso de Google Inc., sus clientes de Google Apps tienen la posibilidad de formalizar con dicha compañía las Cláusulas tipo 2010/87/UE antes indicadas (https://www.google.com/intx/en/enterprise/apps/terms/mcc_terms.html).

d) **Proveedores localizados en otros países:** Deberá considerarse que no ofrecen un nivel adecuado de protección de datos, por lo que se requiere que el Director de la Agencia Española de Protección de Datos autorice la transferencia internacional de datos. Como se ha dicho antes, en estos casos la empresa cliente debe presentar:

1.- Solicitud formal de la autorización.

2.- Copia de las Cláusulas tipo 2010/87/UE firmadas por la empresa cliente y el proveedor, en idioma español. Si el original no se ha firmado en este idioma, deberá presentarse una traducción jurada.

3.- Poder suficiente de todos los firmantes de las Cláusulas tipo 2010/87/UE.

Si el proceso de solicitud de autorización transcurre sin problemas, su concesión puede tardar en producirse hasta tres meses, no pudiendo utilizarse el servicio de correo electrónico hasta obtener la autorización.

En la práctica, **puede resultar harto difícil que determinados proveedores localizados en el extranjero se avengan a facilitar la documentación requerida para solicitar la autorización al Director de la Agencia Española de Protección de Datos.**

El que una empresa empiece a utilizar un servicio de correo electrónico sin haber obtenido previa autorización del Director de la Agencia Española de Protección de Datos para la transferencia internacional de datos, cuando sea necesario, constituye una infracción tipificada como muy grave en el artículo 44.4.d) de la LOPD, **sancionable con multa de 300.001 a 600.000 euros.**

PATRIOT ACT, ley aprobada por el congreso de los EE.UU el 26/10/2001 [6].

Hay que tener en cuenta que dependiendo del país de localización del proveedor, éste puede estar sometido a regulaciones que posibiliten el que determinados organismos oficiales puedan acceder fácilmente al correo electrónico de sus clientes. Este es el caso de la **USA Patriot Act,** que permite al FBI, la CIA, la NSA y las fuerzas armadas estadounidenses acceder al correo electrónico de una empresa española que haya contratado el servicio de correo electrónico con un proveedor estadounidense, a los efectos de llevar a cabo una investigación sobre actividades terroristas.

De hecho, conforme a lo establecido en dicha norma, **el proveedor que reciba la orden de la administración estadounidense para facilitar el acceso al correo electrónico de sus clientes no podrá informar de este hecho a los mismos.**

[6] Texto completo: http://www.justice.gov/archive/ll/highlights.htm

SOBRE INTERBEL

Interbel, especialistas en Email para empresas. Empresa con una experiencia de más de 15 años ayudando a las empresas con soluciones de email, desde herramientas de calidad a buen precio hasta formación y asesoramiento sobre gestión y productividad del email.

El Grupo Interbel tiene una red de 800 distribuidores activos y 4.000 empresas clientes en España y Latinoamérica. Con presencia en Barcelona, Miami, Colombia, México y Argentina, y el respaldo de un gran servicio de asesoría y soporte técnico, garantiza soluciones de correo electrónico para que usuarios y empresas trabajen de modo más productivo con el email y la comunicación. Software, metodología y soluciones que proporcionan la seguridad, productividad y fiabilidad que las compañías buscan en el correo.

Contacto:

Meritxell Solé
Responsable Comunicación
msole@interbel.es
Tfno.: 902 39 39 39
Passeig de Gràcia, 120 3º 1ª
08008 Barcelona

SOBRE DERECHO.COM

El Departamento Jurídico de Derecho.com lleva prestando servicios relacionados con el Derecho de las Tecnologías de la Información y la Comunicación desde 1997.

Actualmente destacan sus soluciones en materia de protección de datos personales; comercio electrónico; revisión legal de páginas web; propiedad industrial e intelectual y resolución de conflictos relacionados con los nombres de dominio en Internet; así como la elaboración y revisión de todo tipo de documentos y contratos mercantiles y tecnológicos

Contacto:

Eric Gracia González
Abogado
eric@derecho.com
Tfno.: 93 317 84 04
Ausiàs Marc 7, 2º
08010 Barcelona