ANÁLISIS

RISKY BUSINESS II: PRIVACIDAD DE DATOS, ERRORES COMUNES Y CONSEJOS PRÁCTICOS

FEBRERO 2024

P·P·O ABOGADOS

RISKY BUSINESS II: PRIVACIDAD DE DATOS, ERRORES COMUNES Y CONSEJOS PRÁCTICOS

1. Introducción

Seguramente, el primer y único momento en que muchas empresas comenzaron a preocuparse por la Privacidad de Datos fue cuando crearon sus sitios web, estableciendo una política de privacidad y un botón para aceptar dicha política. Sin embargo, ante la ausencia de normativa específicas que regule este tema en Bolivia, cada vez más empresas están interesadas en comprender y desarrollar regulaciones internas para la Protección de los Datos que manejan.

Hoy en día, empresas y personas intercambian datos a nivel internacional a diario, a través de diversas plataformas, confiando en que estos datos están protegidos. En ausencia de una norma nacional general, la experiencia y buenas prácticas internacionales, nos ha permitido comprender las necesidades de empresas y usuarios en relación a la gestión de datos y cómo esto puede generar mayor confianza en las interacciones comerciales. Así también, abordamos elementos como la creación de políticas y cómo mitigar los riesgos creados por su ausencia.

Como elemento de apoyo, referimos a la legislación comparada, donde criterios generalmente aceptados pueden llenar los vacíos legales necesarios. Un ejemplo destacado es el Reglamento General de Protección de Datos, normativa Europea que establece directrices sobre el tratamiento de datos de personas físicas. Estos principios nos permiten aplicar conceptos y nociones que serán relevantes para todos los actores, nacionales e internacionales, que recopilen o procesen datos en Bolivia.

En ese contexto, hemos identificado algunos de los errores más comunes en los que empresas y empleados pueden caer, y como evitar que estos sigan sucediendo, guiados por principios internacionales y buenas prácticas globalmente aceptadas.

2. Errores comunes

a. Enviar correos electrónicos a direcciones equivocadas.

Por muy inofensivo que parezca, este es uno de los errores más frecuentes al momento de lidiar con filtraciones de datos o información confidencial. Errores al enviar correos electrónicos a destinatarios incorrectos tienen consecuencias graves para la privacidad de datos. Estos errores comúnmente suceden porque en la agenda de correos electrónicos se escoge como destinatario el nombre de una lista desplegable de contactos o se utilizan opciones de autocompletar, incluyendo a una persona para la cual no se tenía la intención de enviar el correo. El problema surge cuando el correo contiene

información y/o documentos confidenciales que únicamente deberían ser recibidos por la persona interesada y no así por terceros.

Este tipo de divulgación accidental suele dañar la reputación y la confianza en la empresa por parte de los clientes, especialmente si involucra datos confidenciales o personales delicados.

b. Reenvío de cadenas de correos

El reenvío de cadenas de correos, comúnmente hecho a destinatarios fuera de la cadena original, presenta errores comunes y significativos para muchas empresas. La información contenida en la cadena, muchas veces no revisada, puede ser sensible y no relevante para el nuevo destinatario.

Este acto no solo podría resultar en la violación de la privacidad de los participantes originales, sino que también puede ocurrir sin que ellos estén al tanto, generando una falta de control sobre la información compartida.

En otras palabras, al reenviar un correo, existe el riesgo de que la información incluida llegue a manos equivocadas, violando la privacidad de la información de los participantes en el correo, quienes muchas veces no están al tanto del reenvío del correo a terceras personas.

c. Guardar información "por si acaso"

La práctica de almacenar información más allá de lo necesario es recurrente en muchas empresas, generando complicaciones y riesgos de seguridad. Este exceso de retención de datos no solo implica mayores costos de seguridad y almacenamiento, sino que también dificulta la gestión efectiva de documentos. La falta de control puede incurrir en la pérdida de información, lo que provocaría que la misma pueda generar un riesgo de filtración. De igual forma, la falta de acceso eficiente a documentos necesarios es consecuencia común de esta práctica, haciendo que se solicite nuevamente información a clientes, almacenando más de una vez los mismos datos.

d. Enviar información o publicidad sin la aceptación de los usuarios.

Enviar información o publicidad sin el consentimiento de los usuarios constituye una vulneración a la privacidad. En este caso en particular la normativa boliviana, aunque muy limitada, exige el consentimiento expreso para el envío de marketing. Es decir que, la autorización previa de los usuarios para envíos de comunicaciones de marketing debería ser esencial para que las empresas opten por este tipo de acercamiento a sus clientes. De lo contrario, se corre el riesgo de dañar la relación y de enfrentar sanciones legales.

e. No deshacerse de la información de forma correcta

La falta de un proceso para destruir o eliminar adecuadamente la información expone a la empresa a riesgos de filtración de datos y accesos de terceros no autorizados a información confidencial sensible. Sin un procedimiento efectivo, donde se establezca la

forma apropiada de disposición de documentos o archivos digitales, terceros pueden acceder a documentos confidenciales desechados. La implementación de prácticas sólidas de eliminación es esencial para garantizar la seguridad y privacidad de los datos.

3. Cómo mejorar

a. Revisar la lista de destinatarios de los correos antes de ser enviados

Antes de enviar un correo, se debe verificar la lista de destinatarios para evitar enviar el correo a personas equivocadas, esto puede solucionarse programando que el mensaje pueda ser cancelado segundos después de ser enviado, evitando usar la lista desplegable para autocompletar el mail o en caso de que el correo haya sido ya enviado, tratar de recuperar el mismo lo antes posible o contactar al destinatario solicitando que elimine el correo enviado de forma inmediata. Para el presente caso, y con la finalidad de evitar cometer nuevamente este tipo de errores, servirá adoptar una actitud preventiva, guiándonos por el principio de Confidencialidad del GDPR, lo que supone que los datos sean tratados garantizando su seguridad y evitando cualquier ajeno acceda a los mismos.

b. Consideraciones sobre reenvío de información

Para reducir los posibles efectos negativos del reenvío de información a terceros, es necesario considerar si realmente la persona que recibirá el correo debe acceder a esta. En caso de que así sea, lo idea es reenviar únicamente las partes pertinentes y necesarias y eliminar aquellas partes que no sean necesarias para el destinatario. Ello deberá ponernos nuevamente en una actitud parecida a la del punto anterior, preguntándonos si el destinatario estaría autorizado a recibir todos estos datos y si el mismo está al tanto de que debe guardar la confidencialidad e integridad de los mismos.

c. Limitar la información almacenada, guardar solo lo que realmente sea necesario.

Una práctica que puede ayudar a las empresas a reducir la cantidad de información guardada y que no es necesaria, es limitar la información que se almacena bajo el principio de exactitud, minimización de datos y limitación de la finalidad. Estas nociones implican que los datos guardados sean exactos, limitados y pertinentes al fin que se persigue con el tratamiento de los mismos, y que el uso de estos suponga la consecución de un fin determinado, no siendo posible posteriormente utilizar tales datos en otras circunstancias.
Asimismo, en la práctica, se deben establecer prácticas de almacenamiento de información, limitada a un fin específico, y verificar en periodos determinados tiempo si es necesario mantenerla o eliminar la misma si es que ya no es requerida.

d. Verificar si contamos con autorización expresa de los usuarios para recibir publicidad

Para dar cumplimiento con la normativa boliviana, es necesario que toda empresa cuente con la autorización de las personas a quienes está dirigida la publicidad, bajo el principio de licitud, para enviar comunicaciones con contenido publicitario. En tal sentido, la empresa deberá solicitar el consentimiento para realizar este tipo de actividades y capacitarse sobre la normativa vigente en materia de Protección a la Privacidad, a la luz de una responsabilidad proactiva respecto al cumplimiento de tales normas.

e. Generar prácticas adecuadas de eliminación de información

Desde conseguir los adecuados recursos (ej: trituradora de papel), hasta implementar una política para la eliminación de información, la realidad de cada empresa podrá ser distinta de acuerdo con su giro empresarial. Sin embargo, para minimizar el riesgo de que terceros accedan a este tipo de información se debe atender en una primera fase al cumplimiento del plazo de conservación necesario y en una segunda fase, prestar especial atención al proceso de "desecharla" de forma tal que ningún tercero pueda reconstruir en todo o en parte la misma.

La ausencia de normativa específica sobre privacidad de datos en Bolivia ha llevado a un aumento en la preocupación de las empresas por comprender y desarrollar regulaciones internas para la protección de la información que manejan. Ante tal ausencia, es necesario identificar principios clave que pueden ser aplicados por empresas nacionales e internacionales en Bolivia tomados de experiencias externas, para poder, desde la iniciativa privada, salvaguardar la privacidad de las personas en territorio nacional.

En este artículo, se han destacado algunos errores comunes que pueden comprometer la privacidad de los datos, desde enviar correos electrónicos a direcciones equivocadas hasta almacenar información innecesaria, también se ha incluido algunas recomendaciones básicas para mejorar la gestión y el tratamiento de datos, en este sentido es esencial adoptar prácticas preventivas y proactivas, como la revisión cuidadosa de la lista de destinatarios, la consideración cuidadosa al reenviar información y la limitación de la información almacenada. Es necesario destacar la importancia de obtener el consentimiento expreso de los usuarios para el envío de publicidad y la implementación de prácticas sólidas de eliminación de información. Al seguir estas sencillas pautas, las empresas pueden empezar a dirigir sus políticas hacia un cumplimiento internacional de regulaciones sobre privacidad, fortaleciendo la confianza de los clientes y mitigando los riesgos asociados con la privacidad de datos en el entorno empresarial boliviano.

Sobre PPO

PPO es la firma de abogados más grande de Bolivia con prácticas líderes en todos los ámbitos. Los clientes saben que pueden confiar en PPO para sus asuntos legales y empresariales más desafiantes. Los 60 abogados de PPO y más de 100 profesionales trabajan asertivamente para brindar un servicio excepcional, asesoramiento sofisticado y soluciones creativas y prácticas.

PPO es la firma de abogados con la mayor cobertura geográfica de Bolivia, con oficinas propias en cinco ciudades: La Paz, Cochabamba, Santa Cruz, Sucre y Cobija.

Autores

Ana Valeria Escobar
Socia
aescobar@ppolegal.com

Fernanda Ribera
Asociada
fribera@ppolegal.com

Contacto

Santa Cruz
Av. San Martín Nº 155
Edf. Ambassador Business Center
Piso 18

La Paz
Av. Ballivián 555
Edif. El Dorial,
Piso 14

Cochabamba
Calle Papa Paulo N°604
Edificio Empresarial Torre 42
Piso 6

Sucre
Calle Ayacucho Nº255
Casa empresarial FEPCH,
Segundo pátio, piso 2

Cobija
Avenida 16 de Julio
N°149
Centro

Teléfono
(+591) 620 02 020