Política de privacidad de datos para Start Ups

¿Porqué es importante y qué tener en cuenta?

La función de una política de privacidad de datos es informar, a clientes o usuarios, para qué y de qué forma se utilizan los datos personales que ellos brindan cuando hacen uso de un servicio, realizan una compra u algún otro tipo de transacción con una empresa.

Los datos personales son información valiosa, la falta de transparencia en su uso o la utilización por quien no tiene autorización para hacerlo, vulnera el derecho a la privacidad de las personas. Por eso, toda empresa que recolecta cualquier tipo de dato personal, con el objetivo que sea, tiene el deber de manejarlos con la mayor transparencia posible informando en forma explícita; quién, cómo y para qué utilizará esos datos.

En general, la política de privacidad de datos debería constar en un documento separado, que en cada caso deberá ser aceptado por los usuarios. En algunos casos, la política de privacidad forma parte de los términos y condiciones generales del uso de un sitio web o un sitio de e-commerce. Cuando esto ocurre, es importante informar a los usuarios que ,al aceptar los términos y condiciones de uso, también están aceptando la política de tratamiento de datos.

Los términos y condiciones de tu sitio o app ¿incluyen una política de privacidad y uso de datos personales? ¿Deberías ajustar los textos de tu política actual para prevenir posibles inconvenientes?

Algunas cuestiones básicas a evaluar al momento de desarrollar, u optimizar, una política de privacidad de datos:

¿Es obligatorio para el cliente proporcionar estos datos? ¿Qué consecuencias tiene proporcionarlos?

Una persona nunca está obligada a otorgar los datos solicitados por la empresa, o aceptar las políticas de privacidad de datos. Sin embargo, una empresa sí puede solicitar al cliente que acepte la política de privacidad y brinde los datos necesarios como un requisito para utilizar el servicio que ofrece.

¿Por cuánto tiempo se conservan estos datos?

El plazo para la conservación de los datos de los usuarios, puede variar, y es definido por cada empresa. Es muy importante que cada compañía defina el lapso de tiempo durante el cuál puede utilizar estos datos, y qué ocurre cuando vence ese plazo. Esto debe estar especificado en la política de privacidad de datos.

Los puntos mencionados, son ítems clave que una política de privacidad de datos siempre debe contemplar para lograr el cumplimiento mínimo del régimen de privacidad de datos.

Por supuesto, puede haber más. Hoy en día, las personas tienen mayor conciencia sobre sus derechos y la importancia de sus datos personales, por lo que es recomendable tener una política de privacidad transparente que explique de manera fácil, ágil y comprensible cómo se recolectan y tratan los datos personales de los usuarios.

¿Qué datos recolecta y trata tu empresa o negocio a través de tu sitio web o app?

En general, los datos que las empresas recolectan en este contexto son: nombre o seudónimo del usuario que utiliza el servicio, número de teléfono, email, DNI, fecha de nacimiento, CUIL o CUIT, y algún otro extra, que varían según el rubro al que se dedique el servicio en cuestión.

La política de privacidad de datos debe detallar absolutamente todos los datos que son recopilados y tratados, y cuáles son sus fines.

¿A través de qué medios se recolectan y tratan estos datos habitualmente?

1º Datos brindados por los usuarios. Son aquellos que el mismo usuario brinda, voluntariamente, al interactuar con la aplicación o página web (completar nombre, alias, direcciones de entrega, etc.).

2º Datos obtenidos a través de cookies u otras tecnología de seguimiento. Las cookies son pequeños archivos con identificadores alfanuméricos, que son transferidos a la computadora de quien utiliza la app o página web mediante el navegador Web, y que permiten a los sistemas de una empresa reconocer su navegador, y decirle cómo y cuándo, las páginas de sus sitios son visitadas. Esta información también debe estar explicitada en la política de privacidad y uso de datos personales a la que el usuario presta consentimiento cuando brinda sus datos.

Aceptación del uso de cookies al ingresar en una web. S bien no resulta indispensable agregar una política específica de cookies y una aceptación al tratamiento de datos vía cookies en momento en el que el usuario accede a tu sitio web, se recomienda hacerlo ya que, de esta manera, se cumple con los más altos estándares sobre privacidad de datos, a nivel mundial.

¿Para qué y cómo se tratan esos datos?

Es fundamental que la política de privacidad indique, en forma explícita, porque se piden esos datos, cómo se lleva a cabo su recolección y cuál es el tratamiento que se les dará.

En general, el objetivo del tratamiento de datos está vinculado con el servicio que se quiere prestar o la comercialización misma de un producto. En cualquier caso, esto debe ser informado al usuario quien deberá, a su vez, prestar consentimiento.

Por lo que se refiere al uso de cookies u otro tipo de tecnologías, que permiten conocer el comportamiento de un usuario o su ubicación al visitar un sitio web, la información obtenido también puede estar ligada a la prestación del servicio, o incluso ser recolectada con fines publicitarios (target marketing). En éstos y en todos los casos, también es necesario obtener el consentimiento del usuario.

¿Qué métodos de seguridad se utilizan para proteger los datos obtenidos?

La seguridad en el tratamiento y conservación de datos, es un pilar fundamentales en lo que se refiere a la protección de datos personales.

Existen diversas tecnologías y métodos de seguridad que permiten proteger las bases de datos. Muchas, incluso permiten gestionar la información de manera diferenciada dentro de una misma empresa, cuidando que no todos sus integrantes accedan a todos los datos, sino sólo aquellos que precisan hacerlo para cumplir sus funciones.

Las empresas deben tomar las medidas de seguridad necesarias para cuidar las bases de datos que conservan y prevenir que los mismas sean robados, modificados o utilizados por alguien que no tenga autorización para acceder a ellos.