Uso responsable de datos personales para Pymes

MAGLIONA ABOGADOS

CNC Cámara Nacional Comercio Servicios Turismo

Indice

La información y los datos personales tienen hoy un altísimo valor como activo intangible para todas las empresas, siendo incluso más importantes que la infraestructura material. Hay responsabilidades éticas, técnicas y legales que las empresas deben aprender a integrar a sus procesos, sin importar su tamaño. Esta guía busca establecer pautas para que ese tratamiento se realice de una manera responsable, dando la confianza necesaria que los datos personales de los clientes se tratarán de una manera segura, transparente y responsable, guiando a las PYMES en este nuevo camino hacia la protección de datos.

Nicolás Yuraszeck, Magliona Abogados

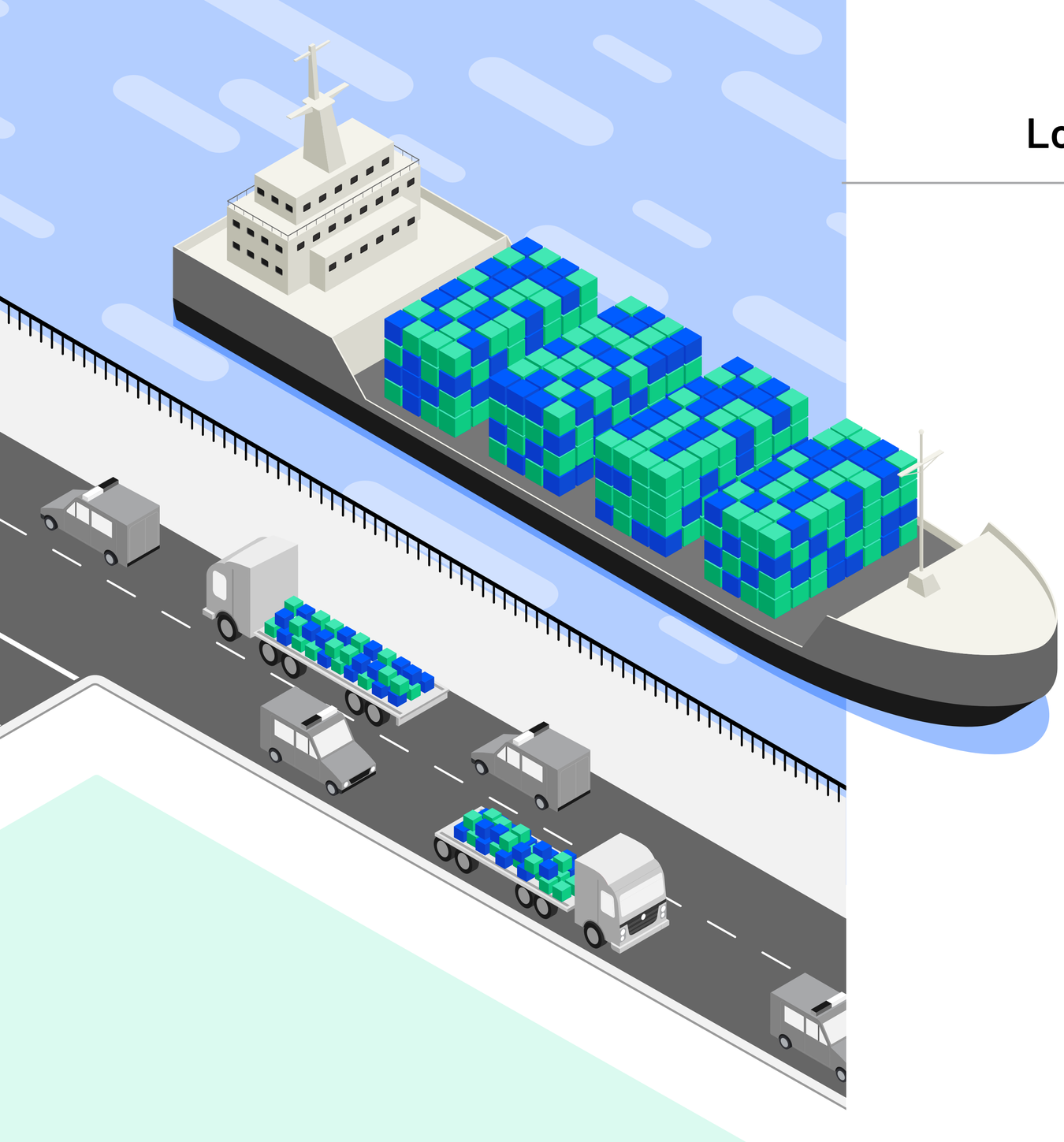
En los tiempos actuales, en que el comercio digital ha adquirido cada vez más relevancia, todas las empresas, sin importar su tamaño, están implementando canales digitales, ya que el comercio electrónico llegó para quedarse y es el complemento necesario del comercio presencial. Es por ello que los datos personales tienen un altísimo valor como activo intangible para las empresas, ya que esta información les permitirá, en especial a las pymes, conocer y fidelizar a los clientes. Pero el manejo de esta información hace que también debamos ser sumamente responsables al tratar adecuadamente estos datos. Pensando en ello es que elaboramos esta guía especialmente para las pymes que están comenzando su digitalización, para que transmitan la confianza necesaria de que la información de los clientes se tratará de una manera segura, transparente y responsable.

Manuel Melero, Cámara Nacional de Comercio.

En un mundo altamente digitalizado, creemos necesario apoyar a las pequeñas y medianas empresas en el salto hacia la digitalización de sus negocios, entregando herramientas, servicios e información que puedan hacerles más fácil este camino y que así la tecnología esté al servicio de la mejora de su gestión. Esta guía busca ser una contribución concreta en la generación de consciencia de la importancia de la privacidad y los datos personales en la digitalización para una mejor relación con el público y los clientes. La reflexión de cara a la transformación digital de las organizaciones no es hoy una opción, es simplemente, un tema de sobrevivencia y hacia allá debemos trabajar de manera colaborativa todos los actores del ecosistema.

Tristán Riquelme, Entel Empresas

Datos



Los datos del 2020

Los datos son la materia prima del Mercado Digital, pueden revolucionar nuestras vidas y crear nuevas oportunidades de crecimiento, especialmente para las pequeñas y medianas empresas. La facilidad con que hoy podemos acceder a grandes cantidades de información gracias al desarrollo de la tecnología tiene cada vez más repercusiones en todos nosotros.

Su correcto uso tiene un efecto transformador en todos los sectores productivos, ya que son un motor fundamental para la economía digital, la cual puede impulsar significativamente la competitividad en el mercado si se establecen las condiciones idóneas que garanticen un marco ético y jurídico.

Por esto surgen leyes y normas que regulan la manera en que se tratan los datos personales, al existir información que las personas desean mantener en una esfera privada o sólo darla a conocer para ciertos propósitos u objetivos.

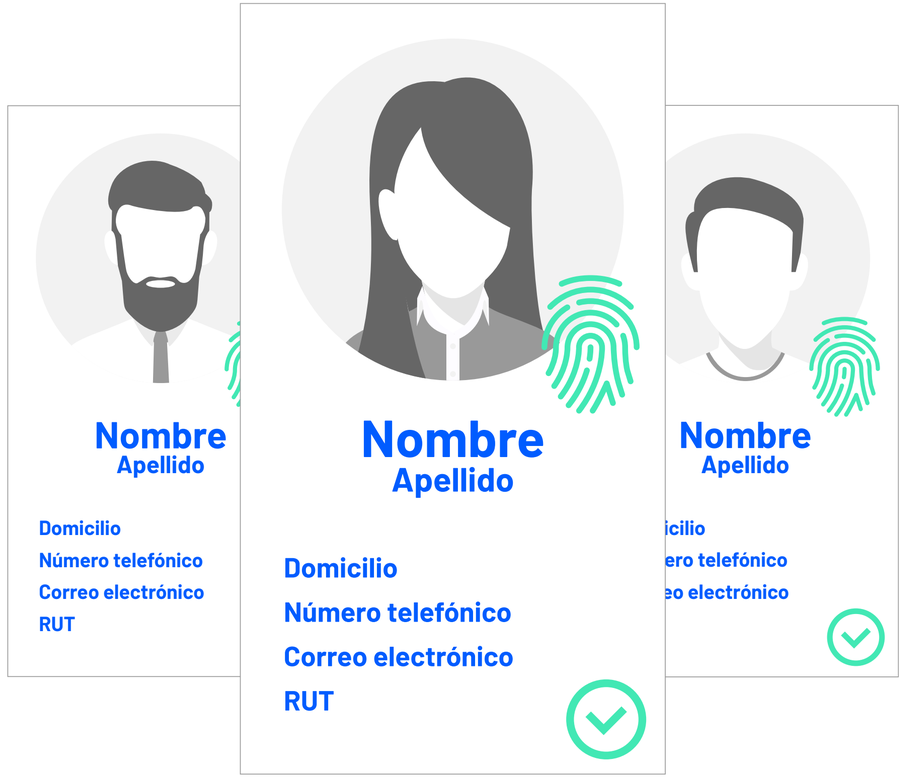
Distintas clasificaciones de un dato

¿Qué es un dato personal?

Datos personales: son toda aquella información que se relaciona con nuestra persona, ya sea, que nos identifique directamente o que nos hace identificables, nos dan identidad, nos describen y precisan.

Ejemplos de lo anterior son:

- **Nombre**
- **Domicilio**
- **Número telefónico**
- **Correo electrónico**
- **Trayectoria académica, laboral o profesional**
- **Número de Cédula de identidad**
- **Entre otros.**



Un dato será personal cuando pueda ser asociado a una persona, mientras que un dato "anonimizado", es cuando se vuelve imposible de asociar a una persona, no pudiendo ser considerado personal.

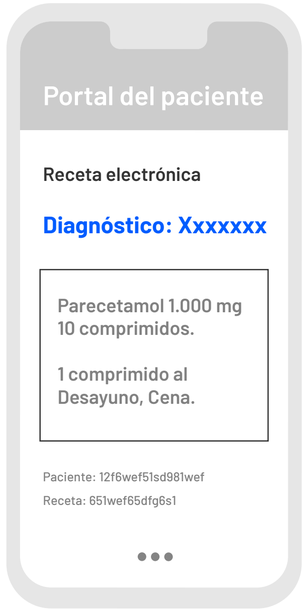
Por ejemplo, el RUT podría ser considerado un dato personal dado que es fácilmente identificable a quién corresponde. Por otra parte, la edad sólo sería un dato personal si es que es posible de alguna forma asociarla a una persona en particular.

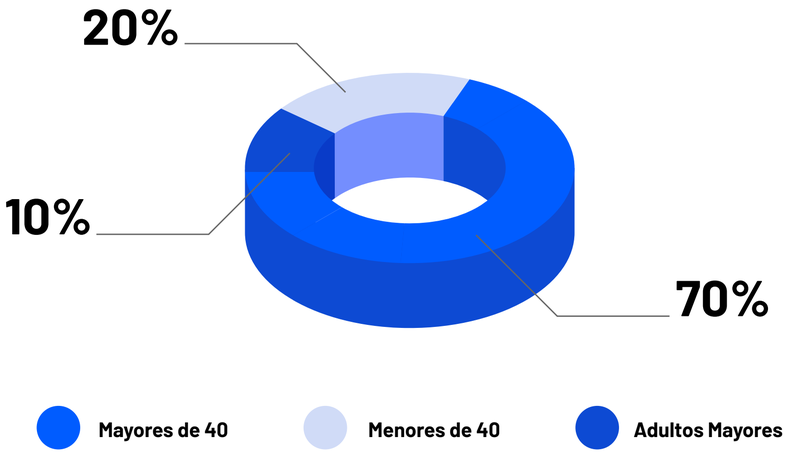
¿Qué es un dato personal sensible?

Es todo dato personal que se refiere a las características físicas o morales de las personas o sobre circunstancias de su vida privada.

¿Cuáles son los ejemplos más comunes? Origen racial, ideologías y opiniones políticas, creencias o convicciones religiosas, estados de salud y su vida sexual.

Ejemplos: Información relacionada a un diagnóstico médico que pueda estar en una receta médica.





¿Qué es un dato agrupado?

Es un dato sobre grupos particulares de personas en función de variables específicas, como edad, profesión o ingresos.

Ejemplo: Personas mayores de 40 años que viven en una determinada comuna.

¿Qué es un registro o base de datos?

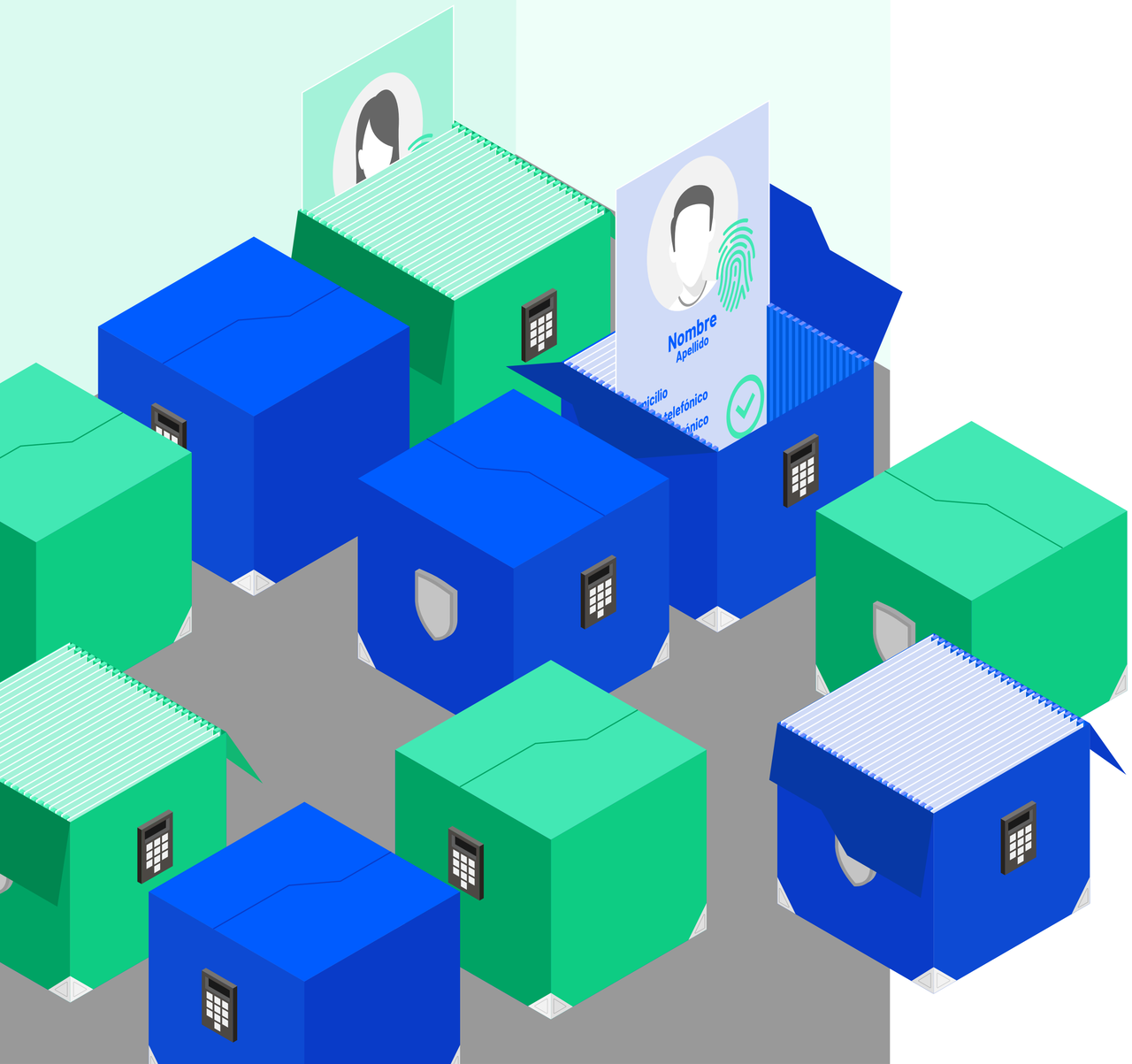
Se trata de un conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

Ejemplo: un listado de asistencia, incluso elaborado a mano, también es un registro o base de datos.

¿Qué entendemos por tratamiento de datos personales?

Cualquier operación o procedimiento técnico, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Principios



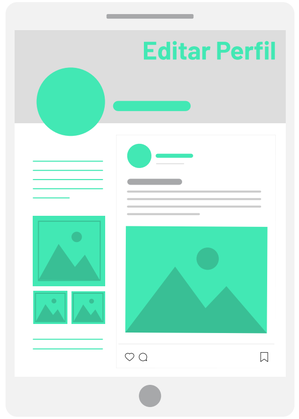
Principios que rigen para la protección de los datos personales y sensibles

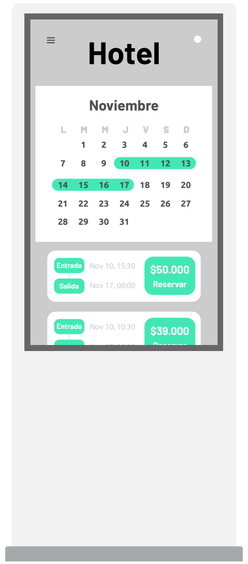
Principio de licitud del tratamiento

Los datos personales sólo pueden tratarse de acuerdo a lo permitido por la ley.

Principio de calidad de los datos

Los datos tratados deben ser exactos, adecuados, pertinentes y no excesivos. Este principio debe observarse durante la recogida y también en el posterior tratamiento de los datos. De este principio, se desprenden a su vez, tres principios rectores:





a. **Principio de Veracidad.**
Los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular, sin necesidad de requerimiento del titular. Por esto se debe:

1. Eliminar los datos caducos
2. Bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda su eliminación; y
3. Modificar los datos inexactos, equívocos o incompletos.

Si un cliente cambia su nombre o dirección, debo ser capaz de corregir dicha información habiendo o no una solicitud del cliente .

b. **Principio de finalidad.**
Los datos personales deben ser recolectados con fines específicos, explícitos y lícitos.

Por ejemplo, una empresa del rubro hotelero no podría utilizar los datos de sus clientes para fines distintos que los de la prestación de los servicios de dicho rubro

c. **Principio de proporcionalidad.**
Los datos personales que se traten deben limitarse a aquellos que sean necesarios en relación con los fines del tratamiento, y deben ser conservados sólo por el período de tiempo que sea necesario para cumplir con los fines del tratamiento.

De acuerdo a lo que señala este principio, sí sería proporcional que una empresa del rubro de la salud solicite datos de salud necesarios para la prestación de sus servicios. En cambio, no sería proporcional que una empresa de venta de autos pida datos de salud del comprador de un vehículo.

Principio de responsabilidad

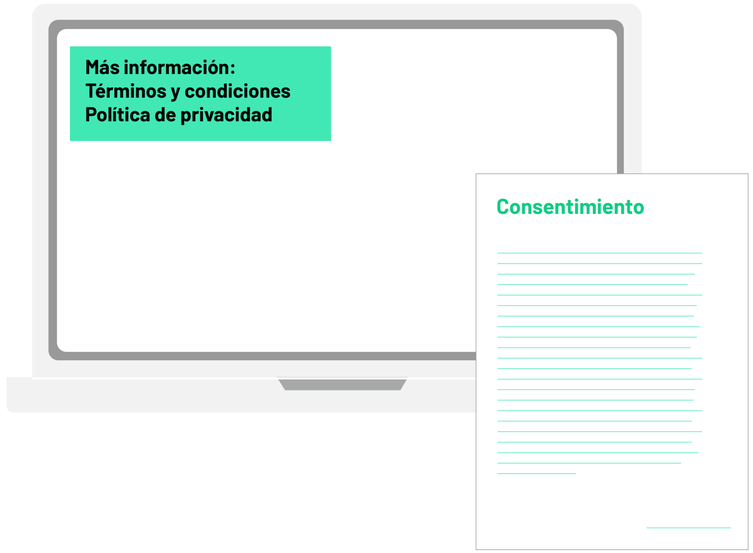
Quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.

Principio de seguridad

Adopción de todas las medidas técnicas, organizativas y de capacitación, de manera continua, que sean necesarias para garantizar la seguridad de los datos personales. Éstas deben ser apropiadas y acordes a la naturaleza de los datos tratados.

Algunas medidas de seguridad posibles de adoptar:

- **Auditorías de seguridad de la información.**
- **Adopción de políticas internas de protección de datos personales.**
- **Establecimiento de políticas de reportes en caso de brechas de seguridad.**



Principio de transparencia e información

Las políticas y prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y ser de fácil acceso para cualquier interesado de manera precisa, clara, inequívoca y gratuita.

Una política de privacidad para clientes debiera indicar los siguientes aspectos:

- **Datos personales que trata la empresa.**
- **Fines del tratamiento.**
- **Periodo de almacenamiento de los datos.**
- **Mecanismo de contacto para el ejercicio de los derechos ARCO por parte del titular.**

Principio de confidencialidad

El responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos.

Según este principio, si no cuento con el consentimiento de mis clientes no es posible comunicar los datos a terceras personas.

Derechos

Derechos de los titulares de datos

La persona, o el consumidor, es el dueño de sus datos personales, no pudiendo renunciar a ello de ninguna forma, ya sea por una cláusula contractual o por políticas de las empresas proveedoras. Esto no debe interpretarse como una prohibición para el tratamiento de los datos personales, sino que es un llamado a hacerlo en el marco de la legalidad, de manera que haya un equilibrio entre la correcta protección a la privacidad y la fluidez de la información en una economía digital, entendiendo que en el desarrollo de la prestación de un servicio la persona habitualmente deberá comunicar a terceros sus datos personales.

La Ley N° 19.628 sobre protección a la vida privada del año 1999, es aquella norma que establece tanto las obligaciones para las empresas (independiente de su tamaño) en el tratamiento de datos personales así como también los derechos de las personas, para la correcta protección de su privacidad.

Estos derechos son conocidos como ARCO: Acceso, Rectificación, Cancelación y Oposición.

Acceso
Rectificación
Cancelación
Oposición

Derecho de Acceso

Consiste en exigir al responsable de tratamiento, la información sobre los datos relativos a la persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

Ej: Cliente ejerciendo su derecho de acceso, llama a una compañía de aplicaciones de transporte, sea que le provea o no el servicio, debiendo ésta:

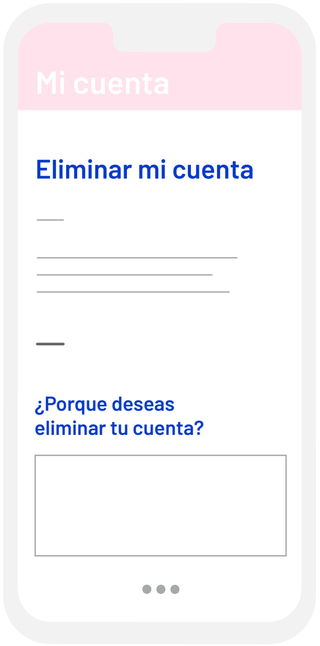
1. **Señalar cuáles son los datos personales que ha recolectado la empresa (nombre, RUT, domicilio, etc)**
2. **La forma en que los obtuvo; y**
3. **Los terceros a los cuales fueron comunicados esos datos (autoridades, empresas relacionadas o proveedores).**

Derecho de Rectificación

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Ej: Cliente tiene derecho, en una forma expedita, a modificar datos que no se encuentren actualizados, como un eventual cambio de nombre o domicilio, que le pudiera afectar en por ejemplo el envío de cobros de servicios básicos (agua, luz, gas, etc.)

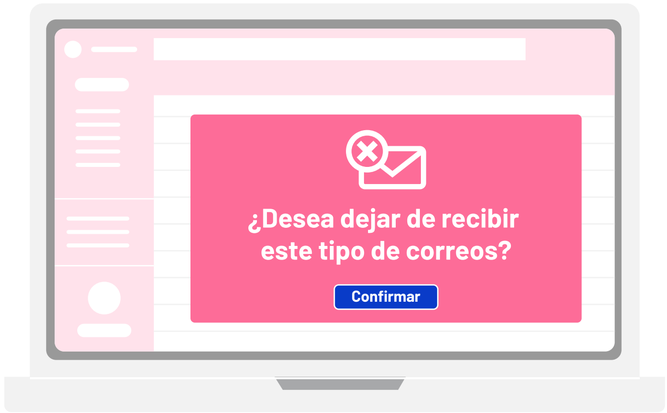
Derecho de Cancelación o eliminación



Exigir que los datos personales se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Ej.: Cliente que entregó su número de teléfono para la facilitación en la entrega de un electrodoméstico comprado en una empresa de retail. Entregado el bien, el dato personal almacenado carece de fundamento legal en virtud del principio de finalidad, por lo que debe ser eliminado ya sea por requerimiento del cliente o por iniciativa de la empresa.

Derecho de Oposición



El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

Ej: Potencial cliente que recibe correo electrónico de publicidad sin su consentimiento, debe tener siempre la opción de de suscripción, para así no recibir más publicidad.

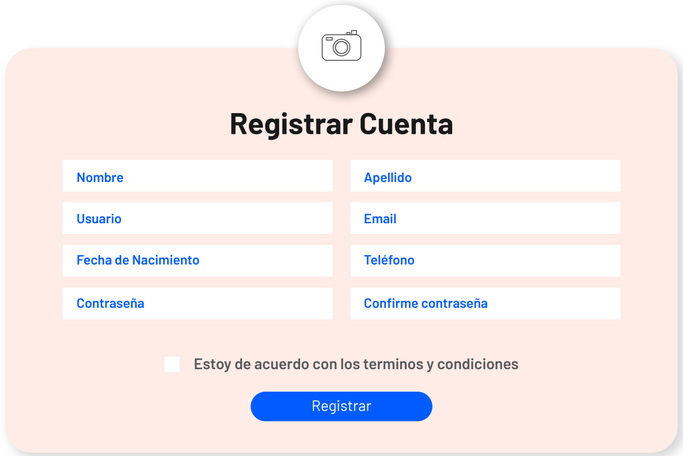
Protección

Protección de los datos

¿Cómo se deben tratar los datos personales de nuestros consumidores?

Como ya hemos señalado, el concepto de tratamiento de datos personales supone las operaciones en todas sus etapas, desde la recolección hasta su eliminación, pasando por su comunicación y anonimización. Es en este proceso, que realizaremos una serie de recomendaciones en cada una de sus etapas, a partir de lo establecido tanto en la ley, especialmente en los principios de tratamientos y obligaciones de las empresas que realizan tratamiento de datos personales, como en las buenas prácticas de la industria.

En cuanto a la recolección de información personal:



En este sentido recomendamos que:

1. La información personal del consumidor sólo debe ser recolectada si la misma es esencial para la transacción, en cualquier otro caso, debe ser optativa en su respuesta, y así informado al consumidor (principio de proporcionalidad);
2. La información sensible no debe ser recolectada sino en casos excepcionales (principio de legalidad);
3. La información debe ser obtenida directamente del consumidor;
4. La empresa debe señalar la finalidad para la cual se hace necesario recolectar la información (principio de finalidad); y
5. La información debe ser recolectada por medios legales y transparentes (en el caso de utilización de cookies establecer política de uso).

En cuanto al uso y comunicación de la información:

En este sentido, recomendamos que:

1. La información personal debe sólo ser utilizada para el propósito para la cual fue recolectada, salvo autorización previa otorgada por el consumidor;
2. La información personal debe sólo ser almacenada durante el tiempo necesario para cumplir el propósito para el cual fue recolectada;
3. La información sensible no debe ser utilizada o comunicada sin autorización previa del titular de dicha información;
4. Si una empresa se disuelve, quiebra, es comprada por otra entidad o de cualquier otra manera cambia su estatuto legal, debe obtener autorización previa del consumidor antes de comunicar la información a la nueva entidad. Si el consumidor no otorga la autorización, la información debe ser borrada; y
5. Las obligaciones anteriormente mencionadas deberían ser igualmente aplicables a cualquier tercera persona que reciba información personal de un consumidor como a la entidad que recolectó la información.

En cuanto al acceso:

En este aspecto, recomendamos que:

1. Las empresas deben otorgar a los consumidores acceso completo y sin costo, a la información que se encuentra almacenada respecto de ellos;
2. Informar a consumidores sobre la existencia de sistemas que pudieran afectar sus derechos a través del procesamiento automatizado de la información, como ocurre en el caso de los comportamientos crediticios (scoring); y
3. Los consumidores deben tener derecho a solicitar la modificación de la información que se encuentre almacenada respecto de ellos, cuando la misma no sea precisa o completa. Los sitios deben explicar claramente cómo los consumidores pueden borrar o corregir sus datos.

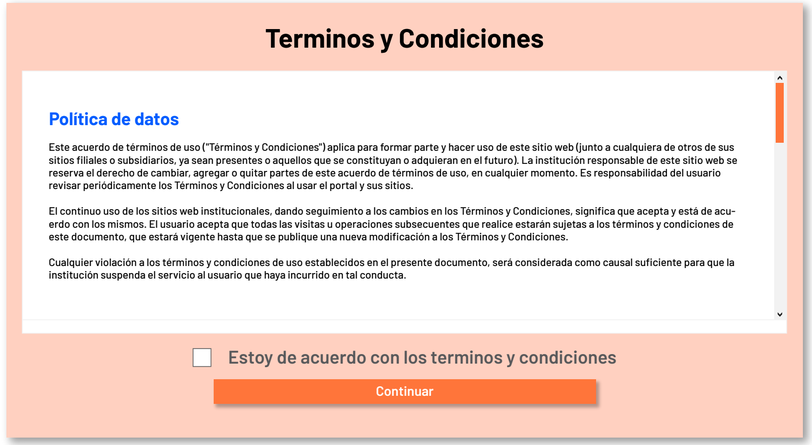
En cuanto a las obligaciones de seguridad

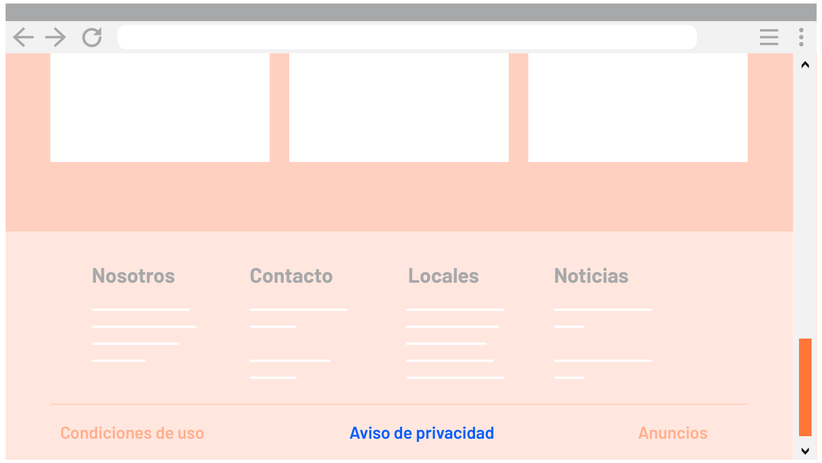
Las empresas tienen la obligación de adoptar medidas administrativas y técnicas para asegurar que la recolección, almacenamiento y comunicación de la información, cuando corresponda, se haga de un modo seguro. Los niveles de seguridad deben estar acordes a la naturaleza de los datos tratados.

En cuanto a las políticas de cumplimiento o compliance

Recomendamos a las empresas

1. Comunicar políticas y prácticas relativas al tratamiento de información personal;
2. Designar a una persona o grupo de personas responsables de la política de cumplimiento por parte de la entidad de los principios sobre protección de datos personales;
3. Contar con canales de reclamos relativos a la política de cumplimiento de los principios de privacidad a la persona o grupo de personas responsables de la misma.





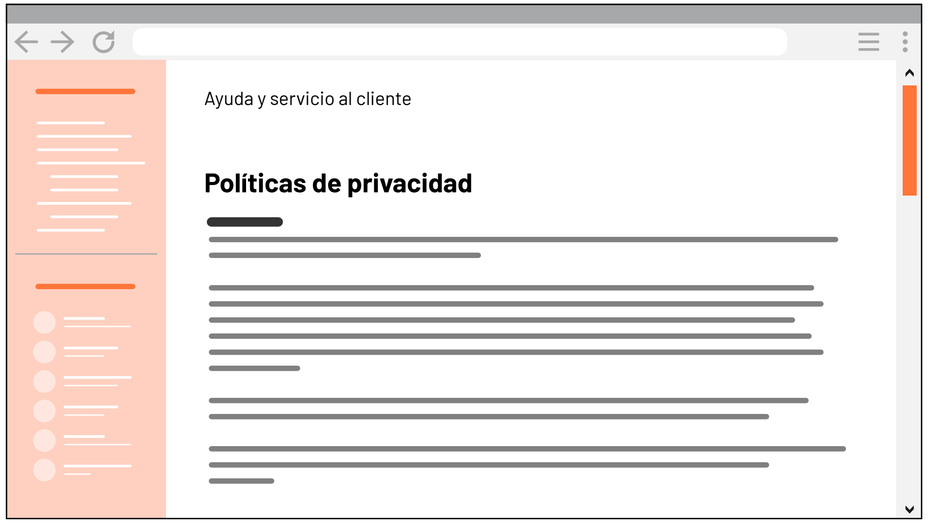
En cuanto a las políticas de privacidad: recomendamos

1. Todos los sitios de comercios que recolecten información de los consumidores deberán proveer una política de privacidad respecto al tratamiento de la información personal;
2. La política de privacidad debe ser exhibida en forma clara y destacada en la página principal del sitio; y
3. La política de privacidad debe estar escrita de una forma clara y precisa para ser entendida.

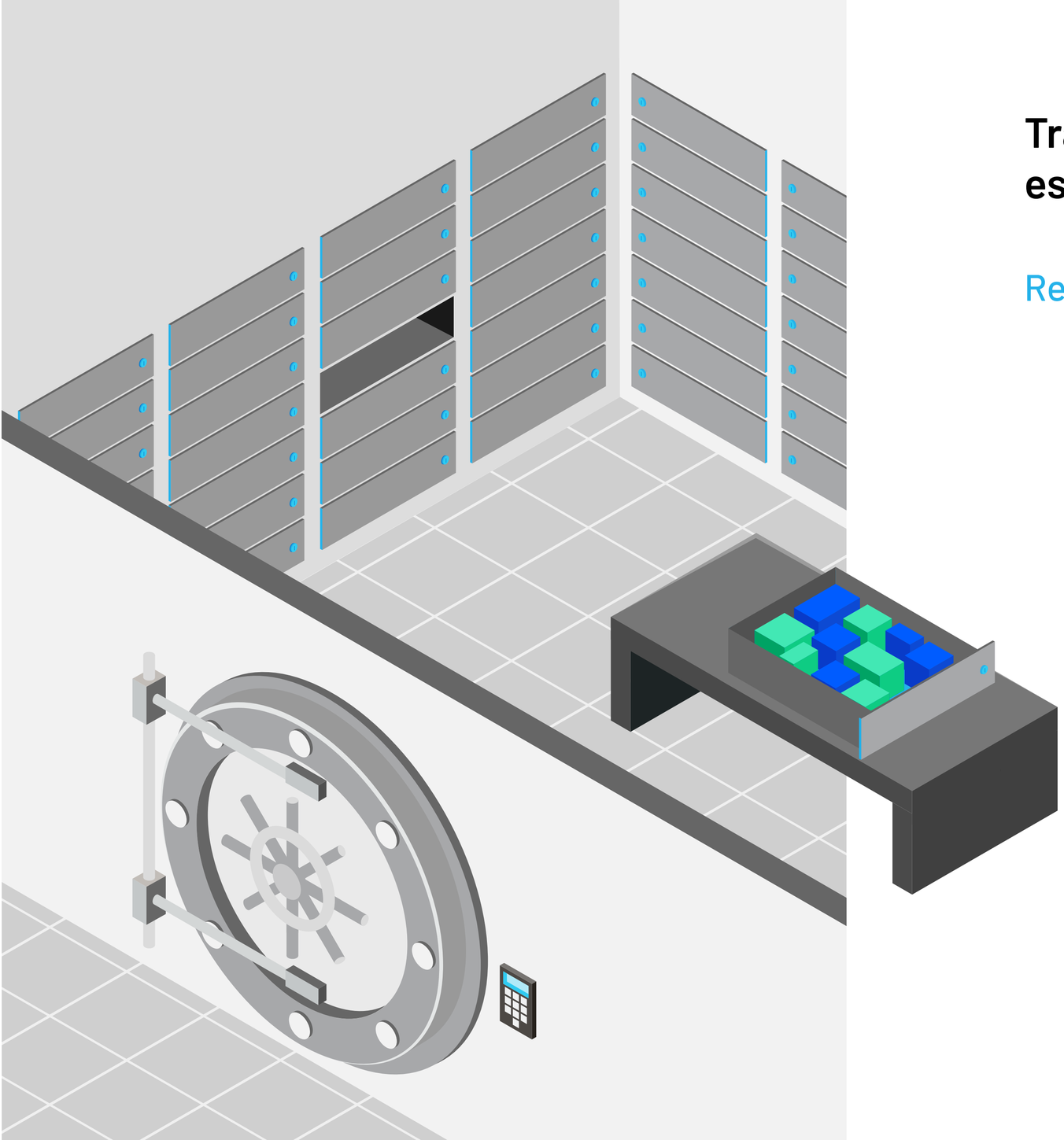
La política de privacidad debería incluir:

La política de privacidad debería incluir:

1. La individualización de la compañía que realiza el tratamiento y que administra el sitio;
2. La naturaleza de la información recolectada;
3. Por qué la información es almacenada y cuál es el uso que se da a la misma;
4. Con qué instituciones la información es compartida (incluyendo sociedades relacionadas, y qué derechos de oposición tiene el usuario al respecto);
5. Criterio de tiempo razonable en cuanto a la información almacenada;
6. Cuáles son los mecanismos de seguridad para evitar intromisiones en el almacenamiento de la información personal;
7. Cómo puede ser modificada la política de privacidad del sitio;



Datos especiales



Tratamiento de categorías especiales de datos

Reserva o secreto bancario:

1. Secreto bancario se refiere a la imposibilidad que toda información referida a depósitos y captaciones de cualquiera naturaleza que reciban los bancos, puedan ser proporcionados a personas distintas que su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente;

2. Reserva bancaria, protección a las demás operaciones y los bancos solamente podrán darlas a conocer a quien demuestre su interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar daño patrimonial a su cliente.

Utilización de datos económicos, financieros, bancarios o comerciales:

Los responsables sólo podrán comunicar información que se refiera a obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas:

1. Consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa;

2. Provengan del incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

Se exceptúa la información relacionada con:

1. Los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario (INDAP) a sus usuarios;

2. La información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentren con alguna modalidad pendiente;

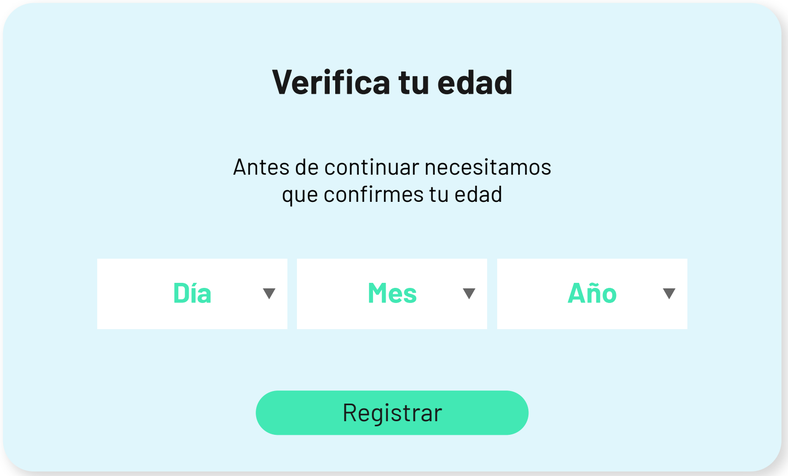
3. Las deudas por servicios de electricidad, agua, teléfono y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura; y

4. Las deudas contraídas con instituciones de educación superior de conformidad a las leyes números 18.591 y 19.287, ni aquellas adquiridas con bancos o instituciones financieras de conformidad a la ley Nº 20.027, o en el marco de las líneas de financiamiento a estudiantes para cursar estudios en educación superior, administradas por la Corporación de Fomento de la Producción, ni alguna deuda contraída con la finalidad de recibir para sí o para terceros un servicio educacional formal en cualquiera de sus niveles;

5. Los protestos y morosidades originados durante el período de cesantía que afecte al deudor.

Datos tributarios

Esta protección consiste en la prohibición de divulgar la cuantía o fuente de las rentas, pérdidas, gastos o cualquier dato relativos a ella, que figuren en las declaraciones obligatorias, impidiendo también que esta información así como sus copias o los libros o papeles que contengan extractos o datos tomados de ellas sean conocidos por persona alguna que sea ajena al Servicio de Impuestos Internos, salvo si fuera necesario para dar cumplimiento a alguna norma legal.



Niños:

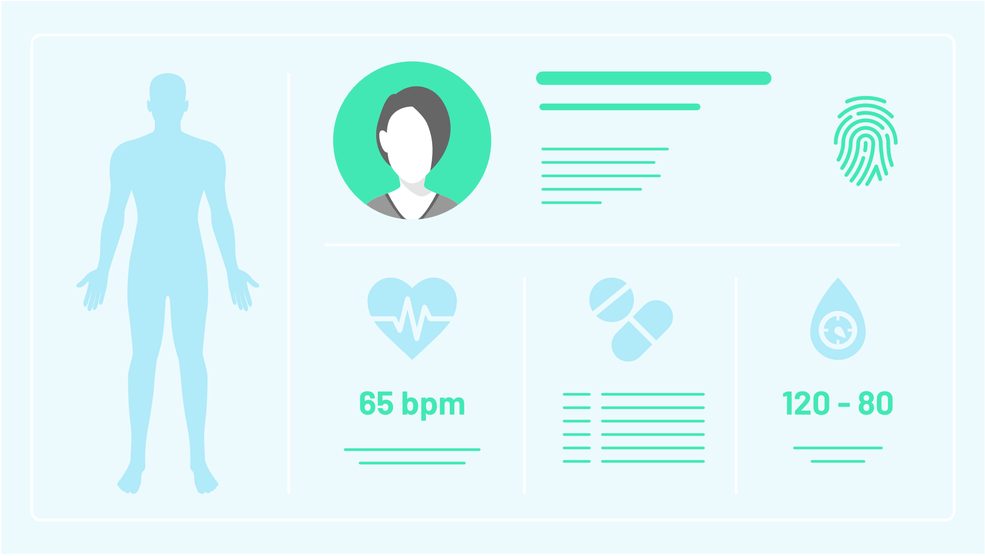
1. No debe solicitarse información personal a los menores de edad (menos de 14 años) o respecto de su familia o cualquier otra persona. La entrega de información no debería ser una condición para poder entrar a un sitio;
2. No deben ofrecerse premios o regalos a los menores de edad por entregar información personal; y
3. No deben utilizarse métodos no transparentes para obtener información personal de menores de edad, como juegos u otros mecanismos.

Datos de salud

Tal como se mencionó anteriormente, los datos relativos a los estados de salud (físicos o psíquicos) de las personas forman parte de los denominados datos sensibles. Debe existir un especial cuidado en el procesamiento de estos datos sensibles, debido a la posibilidad de provocar un grave atentado a la vida privada de las personas debido a su tratamiento.

Por lo anterior, el principio rector del procesamiento de esta clase de datos consiste en la prohibición de que estos sean objeto de tratamiento. La única posibilidad que existe para poder procesar dichos datos, es que una ley expresamente lo autorice, exista el consentimiento del titular de los datos o su procesamiento sea necesario para determinar u otorgar los beneficios de salud que correspondan a sus titulares.

Las recetas médicas, análisis o exámenes de laboratorios clínicos, ficha clínica del paciente y servicios relacionados con la salud son reservados.



Consentimiento para el tratamiento de datos personales

El tratamiento de los datos personales tiene como principio general la libertad en su realización, en la medida que ese tratamiento tenga como base una ley que lo autorice o que el titular consienta expresamente en ello.

Sin embargo, para que exista consentimiento la persona que autoriza, en este caso un cliente del que necesitamos sus datos personales para la venta de un bien o la prestación de un servicio debe:

1. Ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público (principio de finalidad y principio de información); y

2. La autorización debe constar por escrito, pudiendo ser revocada en cualquier momento con posterioridad a su otorgamiento, aunque sin efecto retroactivo (es decir, el tratamiento de todo el tiempo anterior a la comunicación de revocación, seguirá siendo válido), lo que también deberá hacerse por escrito.

Sin embargo, esta regla de requerir el consentimiento por parte del titular no tiene un carácter absoluto y la Ley N°19.628 establece algunas situaciones que exceptúan a una empresa que realiza tratamiento de datos personales para obtenerlos:

1. El tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público (por ejemplo datos obtenidos de Internet);

2. Cuando sean de carácter económico, financiero, bancario o comercial;

3. Cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento (colegios de profesionales);

4. Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (envío de publicidad a correos electrónicos);

5. Las que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos (clubes de esparcimiento social y/o deportivo para su funcionamiento).

En las plataformas digitales, el consentimiento por escrito ha superado la idea de una firma en papel, por el contrario, el completar una casilla o simplemente un “click” cumple el estándar de legalidad exigido, porque supone que la persona que acepta ha sido debidamente informada respecto al tratamiento de datos personales y al mismo tiempo a través de un comportamiento positivo, como lo es el click, declara su conformidad a los términos propuestos en la plataforma, generalmente bajo la forma de políticas de privacidad. Lo anterior sin perjuicio de cumplir con los principios anteriormente mencionados.

Para servicios prestados mediante una plataforma digital el prestador del servicio debe ser capaz de almacenar o registrar el consentimiento de sus clientes, así como también los mecanismos para ejercer el derecho de revocación.

Herramientas

Herramientas y utilidades de seguridad

Considerando el principio de seguridad y su importancia, las empresas que realizan tratamiento de datos personales deberán garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, así como contra su pérdida, filtración, daño accidental o destrucción.

Las medidas de seguridad deben ser apropiadas y acordes con:

1. El tratamiento que se vaya a efectuar;
2. La naturaleza de los datos;
3. El estado actual de la técnica y los costos de aplicación.

Para el logro de lo anterior, las herramientas de seguridad en el tratamiento de datos personales deben ser abordados desde dos niveles distintos:

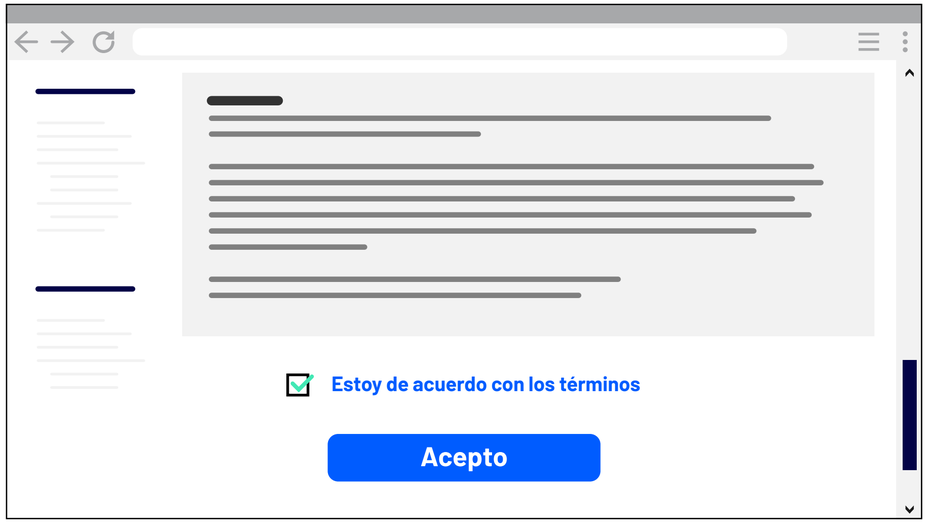
1. Nivel legal.

Se recomienda a las empresas responsables de datos personales:

1. Realizar una revisión que permita incluir o fortalecer las cláusulas de seguridad de la información de los contratos con proveedores a los que se les haya comunicado datos personales de clientes.

2. Comunicar a los clientes, ya sea en contratos o términos y condiciones, las políticas de seguridad que se adoptarán por parte de la empresa.

3. Incorporar en los protocolos internos de la empresa, políticas de seguridad, para establecer en forma clara el actuar desde el correcto uso de las redes e información hasta el modo de actuar ante eventuales brechas de seguridad que involucren datos personales. Lo anterior incorporándolo en los contratos de trabajo de los colaboradores que realicen tratamiento de datos personales en el ejercicio de sus funciones.



2. Nivel técnico

A este nivel, las empresas deberán procurar el uso de herramientas que permitan un uso seguro de los sistemas, que permita hacer una fuerte defensa contra las brechas en materia de datos personales. Estas herramientas ofrecen distintas capas de protección.

Capa básica de protección

Antivirus
Antimalware
Antispyware
Firewall
Copias de Seguridad
Actualizaciones de sistema

Objetivo: Lo que se consigue con estos elementos, será obstaculizar la entrada de archivos maliciosos a los sistemas. También, dentro de sus ventajas está el análisis periódico de los sistemas para localizar vulnerabilidades y remediarlas.

Capa avanzada de protección:

Uso de Seguridad SSL (Secure Sockets Layer o capa de conexión segura)

Objetivo: Al utilizar los protocolos de seguridad SSL, nuestro sistema se coordinará con los elementos anteriores para garantizar una navegación segura con respaldo tanto para el usuario como para el servidor. El método de protección que maneja este elemento es el de encriptación de datos y capa segura de comunicación.

Se utiliza comúnmente en sitios donde se realizará comercio electrónico o sitios relacionados a bancas en línea. Los tipos y precios variarán según la necesidad que el servidor busca cubrir en su plataforma, sin embargo, de no utilizarlo se recomienda que no realice transacciones, ya que se pondrá en riesgo la identidad y el dinero del usuario.

Consideraciones finales

En un mundo cada vez más digitalizado, en el que las personas y consumidores realizan gran parte de sus vidas en línea, los datos personales adquieren una mayor relevancia y valor, ya que permiten el desarrollo de experiencias diseñadas según la necesidad de cada persona.

Al mismo tiempo, los consumidores más conscientes de la importancia y la necesidad de cuidado de ellos, vuelve aún más importante que al momento de usarlos sea para mejorar la experiencia de los usuarios, de manera que vean un valor en el uso de estos.

Por ello, es necesario que la privacidad esté incorporada como elemento central en cada paso del diseño de la experiencia de los clientes, ya que estos valorarán que su información se use para los fines que los entregó y que así se construya una relación de fidelidad y confianza entre el consumidor y la empresa.

Créditos

Contenido y edición

Camilo del Fierro
Paulina Hernandez
Michelle Lister
Claudio Magliona
Eilat Nachari
Daniel Vak
Nicolás Yuraszeck

Diseño y diagramación

Overtone