ManageEngine
ADSolutions

Ebook

Regulaciones sobre la privacidad de los datos y su impacto: un resumen general

Índice

Los datos son la clave para la transformación digital exitosa y con frecuencia se ha observado que las compañías que los manejan y procesan efectivamente superan a las demás. Con un método dirigido por datos, las compañías obtienen la capacidad de tratar con los retos de forma más subjetiva e informada. El análisis exacto de los datos puede también cambiar las estrategias corporativas de ser meramente reactivas a ser predictivas. Más de 2,5 trillones de bytes de datos se generan cada día, y se estima que 90% de los datos del mundo se han recopilado apenas en el último par de años.

De acuerdo con McKinsey Global Institute, es 23% más probable que las organizaciones guiadas por datos adquieran clientes, 600% más probable que los retengan y 19% más probable que sean rentables. Aprovechar los datos eficientemente permite a las organizaciones tomar decisiones informadas y mejorar la experiencia del cliente. Por último, esto resulta en clientes satisfechos que volverán por más.

01 Crecientes preocupaciones sobre la privacidad alrededor del mundo

Durante mucho tiempo, las compañías han recopilado datos de sus clientes sin su completo conocimiento y consentimiento. Ya que el verdadero propósito de la recopilación de esos datos se mantiene oculto de los clientes y se esconde en lo más profundo de los términos y condiciones, muchos clientes hacen clic en la casilla «Aceptar los términos y condiciones» sin entender su impacto.

Ellos han dado mucha de su información a las compañías sin siquiera darse cuenta. Los datos del usuario tienen un valor de mercado enorme, lo que resulta en compañías que agrupan y venden los datos personales de individuos a gran escala. Los sitios web en todo el mundo recopilan y almacenan estos datos de muchas formas:

- Datos personales, incluyendo el nombre, género, dirección IP y ubicación de la persona.
- Datos de captación, como mensajes de texto, correos electrónicos, aplicaciones móviles y páginas de redes sociales.
- Datos de comportamiento, como historiales de compra e información sobre uso de productos.
- Métricas de datos de comportamiento, como satisfacción del cliente, criterios de compra y deseos de productos.

Se ha encontrado que los gigantes tecnológicos en el mundo mantienen más información sobre los usuarios de la que requieren, y con frecuencia dicen usar estos datos para personalizar el contenido y mejorar la experiencia del usuario. Pero el hecho es que estas compañías venden estos datos a anunciantes, publicistas y otros terceros.

Por ejemplo, se comparte un anuncio de rendimiento con respecto a un usuario particular con anunciantes, quienes personalizan sus anuncios con base en el comportamiento de este para hiper enfocarse en él con el fin de atraerlo. La información de ubicación del usuario también se comparte y se usa comúnmente para mostrar anuncios locales personalizados. En respuesta, 86% de los estadounidenses han intentado borrar sus rastros digitales y proteger su información personal que está disponible en línea debido a preocupaciones de privacidad.

El término «dato» se refiere a cualquier información que puede identificar personalmente a alguien. La privacidad de los datos se refiere a protegerlos en términos de su recolección, uso y distribución.

El objetivo es proteger varios tipos de datos, como los datos de primera mano (información que las marcas y creadores recopilan directamente de sus consumidores), los datos de segunda mano (información adquirida de la compañía que la recopila) y los datos de terceros (información comprada de otras fuentes; idealmente incluye datos de distintas fuentes agregados en un solo lugar).

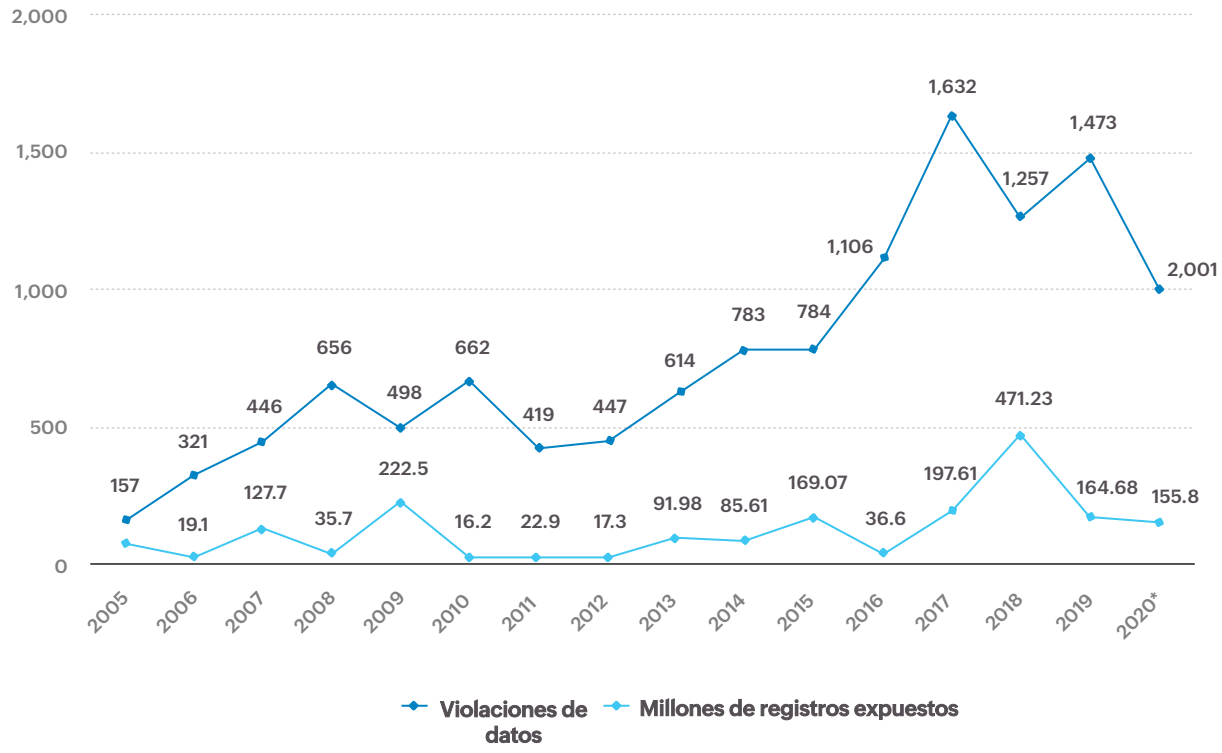
Ya que los consumidores se hacen cada vez más conscientes sobre los derechos de sus datos y cómo se utilizan estos últimos, demandarán estar protegidos. 79% de los estadounidenses han expresado preocupaciones sobre la forma en que las compañías utilizan su información personal. Con la creciente inquietud de la población general sobre el abuso de los datos, hay una necesidad de establecer regulaciones globales de datos que se enfoquen en fortalecer la privacidad de los consumidores y la protección de los datos.

02 Una necesidad urgente de establecer regulaciones sobre la privacidad de los datos

En los últimos años, el abuso de los datos se ha extendido más allá de extraños anuncios que se enfocan en clientes individuales. El aumento en el enfoque de las preocupaciones sobre la seguridad se debe a los numerosos ataques de seguridad informática que han conllevado violaciones masivas de seguridad de los datos personales. Las violaciones de la seguridad de los datos cuestan a las compañías tiempo y dinero. Esta pérdida se da en la forma de pérdida de datos, que se puede compensar en alguna medida, y mediante daños irreversibles a la reputación, lo que en última instancia conlleva la pérdida de consumidores. La lealtad de los consumidores es casi imposible de volver a ganar.

El aumento global de ataques de ransomware es una fuente importante de preocupación para las compañías. De acuerdo con la AICPA, casi la mitad de los estadounidenses espera ser víctima de un fraude el próximo año. Statista estima que el costo global promedio de una violación de la seguridad de los datos en 2021 fue $4,24 millones, un aumento considerable del 10% con respecto al 2020. Con la economía más poderosa del mundo, Estados Unidos es el principal objetivo de ataques cibernéticos y tiene el costo promedio total más alto por violaciones de la seguridad de los datos: $9,05 millones en 2021.

Número anual de violaciones de la seguridad de los datos y registros expuestos en EE. UU. (en millones)



La gráfica anterior detalla el número de violaciones de la seguridad de los datos y los registros expuestos en EE. UU. desde 2005 a 2020. Estos ataques sirven como un recordatorio urgente sobre la necesidad de establecer regulaciones globales sobre la privacidad de los datos. Dichas violaciones de la seguridad de los datos a gran escala, resultantes en la pérdida de información sensible, dinero y, algunas veces, la vida, han impactado a los países alrededor del mundo.

Por tanto, los gobiernos están empezando a regular la recopilación y la gestión de datos por parte de las compañías. Ya que la Declaración Universal de los Derechos Humanos de la Organización de las Naciones Unidas ha declarado que la privacidad es un derecho fundamental, hay una obligación inmediata de preservar los derechos de privacidad.

03 Regulaciones sobre la privacidad de los datos

Con el fin de aumentar las medidas de privacidad y seguridad alrededor del mundo, los distintos gobiernos han empezado a aprobar leyes para controlar los tipos de datos que se pueden recopilar sobre los usuarios, cómo se pueden usar y cómo se deben almacenar y proteger. Estas regulaciones están diseñadas para permitir a los consumidores controlar sus datos.

Una obligación importante es pedir el consentimiento de los clientes cada vez que se recopilen datos. Asimismo, los términos y condiciones deben ser fácilmente entendibles para los clientes. Estas leyes requieren que las compañías permitan a sus usuarios el derecho de acceder a sus datos, tomarlos y usarlos en otro lugar, y solicitar que las compañías borren sus datos personales completamente de sus registros.

Más de 137 países han implementado leyes de privacidad de datos para evitar el abuso de datos personales. He aquí algunas de las regulaciones sobre la privacidad de los datos más importantes alrededor del mundo:

GDPR

i. Reglamento general de protección de datos (GDPR)

Considerada una de las regulaciones de privacidad más prominentes, el GDPR se aprobó en 2018. Impacta todas las organizaciones que procesan datos personales y operan dentro, o que venden productos a la UE. Según la definición del GDPR, el tratamiento de datos también cubre los posibles tipos de uso y procesos involucrados, tales como recopilación, recuperación, almacenamiento, alteración y destrucción de datos.

El GDPR también requiere evaluaciones sobre el impacto de la protección de datos para cualquier tratamiento que pueda suponer un riesgo para los derechos del titular de los datos. Con el fin de limitar la recopilación de datos en la fuente misma, el GDPR enfatiza en la minimización de datos, limitación de propósito y de almacenamiento. Infringir las directrices puede resultar en multas de hasta €20 millones o hasta el 4% de las ventas globales totales de la compañía del año fiscal anterior, lo que sea mayor.

CCPA

ii. Ley de privacidad del consumidor de California (CCPA)

La CCPA cubre a los residentes de California y aplica a compañías con ingresos brutos anuales de más de $25 millones; aquellas que compran, reciben o venden información personal de 50 000 o más residentes, hogares o dispositivos, y aquellas que derivan 50% o más de sus ingresos anuales de vender información personal de los residentes.

La CCPA requiere que las compañías emitan un mensaje de «notificación de recopilación» que informe a los clientes sobre la recopilación de su Información personal y su propósito. También tiene una sección completa sobre la regulación del funcionamiento de los corredores de datos. Infringir las regulaciones puede resultar en multas desde $2500 por una violación no intencional a $7500 por una violación intencional.

CPRA

iii. Ley de derechos de privacidad de California

Introducida en 2020 como una versión más integral de la CCPA, la CPRA busca aumentar los derechos de los consumidores en términos de la privacidad y seguridad de los datos. Con una nueva categoría llamada información personal sensible (SPI), la CPRA demanda que las compañías proporcionen protección adicional con base en la sensibilidad de la información personal. Esto incluye requisitos de divulgación actualizados, de limitación de propósito y de inclusión y exclusión voluntarias.

Además de la expansión de las leyes en la CCPA, la CPRA introduce cuatro nuevos derechos para los consumidores: el derecho a corregir información personal imprecisa, el derecho a limitar el uso y divulgación de la SPI, el derecho a acceder a la información sobre toma de decisiones automatizadas y el derecho a excluir la tecnología de toma de decisiones automatizadas. Estos nuevos derechos protegen a los usuarios contra el abuso de datos por parte de tecnologías guiadas por IA.

Además de estas regulaciones, hay otras leyes con respecto al derecho de los clientes y la recopilación de los datos. La Ley de responsabilidad y portabilidad del seguro de salud (HIPAA) controla la industria sanitaria y evita la recopilación e intercambio ilegal de la información sanitaria de los pacientes sin su previo consentimiento. La Ley Gramm-Leach-Bliley (GLBA) se aplica a instituciones financieras para garantizar la seguridad y privacidad de la información financiera de los clientes con respecto a sus préstamos, estados financieros, transacciones y más.

El Estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS) garantiza transacciones con tarjetas de crédito protegidas y legales. La Ley de informe justo de crédito (FCRA) regula la recopilación y uso de la información crediticia de las personas. Con el fin de garantizar la seguridad de los niños, la Ley de protección de la privacidad en línea para niños (COPPA) controla la recopilación de información sobre menores.

04 El impacto de las regulaciones sobre la privacidad de los datos en las compañías

Las regulaciones sobre la privacidad de los datos permiten a las compañías optimizar sus prácticas de manejo de datos y facilitar transacciones digitales transfronterizas. Pero requieren que las compañías fortalezcan sus tecnologías para la gestión de datos con el fin de compilar robustas funciones digitales. La idea principal es crear modelos corporativos conformes y eficientes que protejan la privacidad de los datos de los clientes.

Hay dos cambios importantes que las compañías pueden esperar como resultado de las regulaciones sobre la privacidad de los datos. Primero, la privacidad se volverá una expectativa fundamental entre los clientes. Segundo, la transparencia en las políticas de privacidad no será opcional. Ya que los clientes se hacen cada vez más conscientes sobre las políticas de datos y los gobiernos aplican requisitos de privacidad, las compañías están aprendiendo que implementar dichas políticas puede crear una ventaja comercial al mantenerse a la vanguardia.

Por otro lado, desde una perspectiva corporativa, el costo del cumplimiento se disparará, ya que las organizaciones podrían tener que asignar recursos humanos y financieros aparte para cumplir estas regulaciones. Con las elevadas sanciones por incumplimiento y el posible riesgo de perder su valor de marca, las organizaciones se verán forzadas a pagar para lograr el cumplimiento. El otro impacto sobre las compañías es la sobrerregulación de las políticas. Los clientes se saturan con interminables formularios de consentimiento para cada proceso de datos, lo que dificulta el uso de plataformas en línea.

Con la amplia implementación de regulaciones alrededor del mundo, las compañías están en riesgo de incumplir y aumentar la inversión. Muchos marcos se han desarrollado para ayudar a las compañías a encontrar la combinación correcta de inversión óptima y cumplimiento de las regulaciones. El marco de gobernanza sobre la seguridad de los datos de Gartner describe cómo las compañías pueden cumplir sus requisitos legales mientras tratan con los datos de los clientes.

El marco sugiere los siguientes pasos:

- Identificar y enfocarse en los datos que se ven afectados por las regulaciones sobre el cumplimiento de la privacidad de los datos.
- Desarrollar evaluaciones de impacto para la protección de datos y administrarlas periódicamente mientras se mantiene a todos los interesados de la compañía involucrados.
- Configurar controles de tecnología para disminuir el riesgo a un nivel aceptable.
- Revisar sistemáticamente las políticas de seguridad y cuando sea que los riesgos de la compañía cambien.

05 La relación entre las regulaciones sobre la privacidad de los datos y la IAM

Las regulaciones sobre la privacidad de los datos han cambiado fundamentalmente la forma en que las compañías tratan la información personal de los clientes. Se debe proteger cualquier información que pertenezca a una persona y que se pueda usar para identificarla. El objetivo último es evitar el abuso de los datos personales al monitorear la recopilación de datos y evitar violaciones de la seguridad de los datos. Con la constante expansión de las compañías, se hace más difícil garantizar el cumplimiento de todas las leyes.

i. Cumplir en todo momento con las regulaciones sobre la privacidad de los datos utilizando la IAM

Las soluciones de IAM dan a las compañías funciones de seguridad altamente confiables para ayudarlas a cumplir los estrictos requisitos de cumplimiento de las leyes sobre privacidad. Con la IAM, las organizaciones pueden cumplir fácilmente las estrictas obligaciones y evitar tratamientos ilegales cuando se manipulan datos privados de los clientes. Una solución centralizada de IAM da medidas de seguridad como MFA, PAM y políticas de acceso basadas en la organización. A través de estas, las compañías pueden garantizar que solo usuarios autorizados accedan a datos sensibles.

Además, las funciones como la autenticación basada en roles y los métodos de privilegios mínimos fortalecen el acceso interno dentro de la compañía. Las funciones federadas de autenticación ayudan a dar y revocar el acceso, una función que resulta útil durante la incorporación de nuevos empleados y trabajadores temporales. Se pueden implementar las opciones de codificación avanzada y las medidas de protección ante amenazas dadas por las soluciones de IAM para salvaguardar los datos almacenados on-premise y en la nube.

Ya que las leyes sobre privacidad de datos se renuevan para cubrir operaciones centradas en la nube, dichas funciones ayudarán a gestionarla compañía con una mínima interrupción de las operaciones. Las soluciones de IAM también están diseñadas para combatir varios tipos de ataques cibernéticos, tales como phishing, malware, virus y ataques de DDoS. Por tanto, las compañías con soluciones de IAM implementadas para gestionar y dirigir sus procesos de seguridad serán capaces de cumplir en todo momento correctamente las leyes de privacidad de los datos.

ii. El impacto de las regulaciones de privacidad de los datos en la evolución de las soluciones de IAM

Con la introducción de regulaciones estrictas sobre la privacidad de los datos, las soluciones de IAM necesitan evolucionar para cumplir con sus requisitos. Una de las razones por las que las leyes sobre privacidad de datos son relevantes para el desarrollo ético de las soluciones de IAM es que algunos factores como las credenciales del usuario se basan en información personal del usuario, como huellas digitales, ubicaciones geográficas y funciones de dispositivos personales.

Si una organización escoge adoptar una solución de IAM, es de absoluta necesidad que garantice el cumplimiento de todas las leyes sobre privacidad de los datos desde la etapa de desarrollo. Mientras que las funciones como MFA y PAM dan seguridad a nivel de usuario, los protocolos que las ejecutan desde el modo administrador también utilizan algoritmos avanzados y técnicas de codificación para mantener la seguridad. Todos los procesos y aplicaciones deben parchearse y actualizarse.

iii. Qué debe tener una solución de IAM para cumplir en todo momento

Al desarrollar y actualizar las soluciones de IAM, se deben tener en consonancia con las leyes pertinentes sobre privacidad de datos para cumplir en todo momento. He aquí algunos puntos que la compañía debe considerar para crear legalmente soluciones de IAM sostenibles:

Garantizar la privacidad de los datos y el cumplimiento de seguridad desde el inicio de la etapa de desarrollo y reevaluar de manera integral el tiempo de vida del producto.

En términos de la recopilación y gestión de los datos personales de los clientes, recopilar solo lo que es necesario y mantenerlos solo el tiempo necesario. Proteger el almacenamiento y la eliminación de los datos es igualmente importante. Garantizar que solo puede acceder a dichos datos sensibles quien necesite hacerlo.

Garantizar la privacidad de los datos y el cumplimiento de seguridad desde el inicio de la etapa de desarrollo y reevaluar de manera integral el tiempo de vida del producto.

En términos de la recopilación y gestión de los datos personales de los clientes, recopilar solo lo que es necesario y mantenerlos solo el tiempo necesario. Proteger el almacenamiento y la eliminación de los datos es igualmente importante. Garantizar que solo puede acceder a dichos datos sensibles quien necesite hacerlo.

06 La gestión de cambios propiciada por las regulaciones sobre la privacidad de los datos

La confusión frecuente sobre las regulaciones sobre la privacidad de los datos es que solo impactan al departamento legal. Pero el punto que con frecuencia se omite es que todos los que trabajan con datos en una compañía deben ser conscientes de las regulaciones y cumplir en todo momento. Muchos expertos que estudian estas regulaciones proponen que esto tiene menos que ver con la gestión de datos y más con los procesos de gestión de cambios. Las compañías deben repensar y restructurar la forma en que manejan los datos de los clientes. La mejor forma de implementar estas regulaciones de privacidad en una compañía es implementar la gestión de cambios.

Invertir en análisis y tecnologías de automatización debe ser el primer paso de cualquier compañía hacia la construcción de un sistema robusto y conforme que garantice la adherencia a todas las regulaciones de privacidad. La mayoría de las leyes sobre privacidad de datos mencionan los derechos de acceso de los clientes, lo que significa esencialmente que un cliente puede, en cualquier momento, solicitar una copia de todos los datos que se recolectan o que se eliminan.

Las compañías necesitarán soluciones digitales automatizadas para cumplir con estos requisitos eficientemente. Por ejemplo, los formularios que llenan automáticamente los detalles necesarios, las herramientas de guía de desktop o los asistentes virtuales agilizarán el proceso con un esfuerzo manual mínimo. Esto, a su vez, reducirá la posibilidad del abuso de datos.

Las siguientes son algunas prácticas que las organizaciones deben seguir para gestionar eficientemente los cambios que las regulaciones generan:

- Para garantizar el cumplimiento de todas las leyes pertinentes, las organizaciones deben tener un conocimiento actualizado de estas. Emplear asesoría legal para este fin permitirá rendir cuentas e implementar un proceso riguroso.

- Auditar constantemente y evaluar los controles de la compañía es esencial para generar un sistema que pueda resistir ante los complejos cambios en las regulaciones de privacidad.

- Toda organización es única y, por tanto, no hay una solución que pueda aplicarse a todas. Es crucial para las compañías entender la naturaleza de los datos que maneja y sus deberes antes de intentar buscar una solución. Lo que funciona para una compañía en una industria puede no funcionar en otra.

- Otro factor importante que se debe considerar es la ubicación de los clientes. Cada país o jurisdicción tiene leyes locales específicas, y también es obligatorio cumplir con todas ellas.

- Las compañías deben garantizar que estas regulaciones de privacidad se añaden a sus valores centrales. Con dicho cambio cultural establecido, se considerará la privacidad justo desde el inicio de cada nuevo proyecto y se le hará seguimiento hasta el final.

- Las compañías deben alejarse del método tradicional para la recopilación de datos en que tratan de obtener y almacenar tantos datos de los clientes como sea posible. Ya que las regulaciones se hacen más estrictas, las compañías deben recopilar, manejar y almacenar solo lo requerido. Se debe emplear la idea de una recopilación minimalista de los datos. Asimismo, la eliminación de datos después de su vencimiento o de su uso es igualmente importante para cumplir con las regulaciones de privacidad.

- Las organizaciones deben ser transparentes con respecto a los datos personales recopilados de sus clientes y gestionar solicitudes para la eliminación de datos con el fin de garantizar el cumplimiento legal.

Las siempre cambiantes leyes globales sobre privacidad de datos solo se harán más estrictas con el paso del tiempo. El paso ideal que debe tomar cualquier compañía sería cumplir voluntariamente con todas las leyes de privacidad en las ubicaciones donde sus negocios operan. Además, también se deben tener en cuenta los países y estados afectados indirectamente por sus compañías tal como lo requieren las regulaciones como el GDPR. Con el fin de evitar costosas multas, interrupciones operativas y la pérdida de los clientes, entre más pronto las compañías planeen y cumplan con estas leyes, más exitosas serán.

Acerca de AD360

AD360 es una solución para la gestión de identidades y accesos (IAM) para gestionar las identidades de los usuarios, controlar los accesos a los recursos, reforzar la seguridad y garantizar el cumplimiento. AD360 ofrece todas estas funcionalidades para Windows Active Directory, Exchange Server y Office 365. Con AD360, usted puede escoger los módulos que necesita y comenzar a afrontar los retos de IAM en entornos on-premises, en la nube e híbridos, todo desde una sola consola.

Para más información sobre AD360, visite:

https://www.manageengine.com/latam/active-directory-360/

$ Obtenga una cotización

Descargar