elastic

Uso de Elastic para impulsar el cumplimiento de las leyes de privacidad de todo el mundo.

Resumen ejecutivo

Para operar con éxito en el mundo digital moderno, las organizaciones se centran en los datos, especialmente en su papel en la IA. En respuesta, una explosión de leyes y regulaciones de privacidad está cambiando el panorama empresarial en todo el mundo. Mantenerte al día con estos cambios normativos no solo sirve para reducir y mitigar el riesgo, sino que también es un factor diferenciador clave y poderoso en el mercado, donde el cumplimiento de la normativa legal y regulatoria en materia de privacidad, en constante evolución, puede aumentar la confianza de los clientes, impulsar el crecimiento financiero y reforzar la resiliencia operativa.

Este documento técnico introduce conceptos esenciales en la legislación de privacidad de datos y demuestra cómo las organizaciones pueden desplegar la poderosa plataforma de Elastic no solo para cumplir con los requisitos de datos personales, sino también para aplicarlos con rapidez, eficiencia y confianza. Expondremos los seis principios fundamentales de privacidad que son ampliamente aplicables a las regulaciones de privacidad de datos en todo el mundo y los asignaremos a las soluciones de la plataforma de Elastic, ayudando a las organizaciones a convertir la privacidad de los datos de una obligación de cumplimiento en una ventaja competitiva.

Ten en cuenta lo siguiente: este documento técnico se proporciona solo con fines informativos y no pretende constituir asesoramiento legal. Consulta a tu propio asesor legal para obtener asesoramiento legal.

Antecedentes e introducción a las leyes de privacidad en el mundo

Las leyes de privacidad plantean retos cada vez más complejos a las organizaciones que recopilan datos personales. Dado que los datos personales se consideran uno de los bienes más valiosos del mundo, el cumplimiento de las leyes de privacidad puede ser un importante motor de negocio para las empresas, y su incumplimiento puede obstaculizar significativamente el crecimiento de una compañía.

A medida que las organizaciones recopilan más datos personales, encontrar una solución escalable para gestionar y proteger esos datos se vuelve cada vez más importante para demostrar su responsabilidad y construir una reputación positiva como proveedor de confianza en un mundo cada vez más consciente de la privacidad.

Si bien existen distinciones entre varias leyes de privacidad, muchas de ellas comparten ciertos principios generales.

Las principales leyes de privacidad incluyen:

- El Reglamento General de Protección de Datos de la UE (“RGPD”) y su análogo del Reino Unido
- Leyes de privacidad estatales de EE. UU., como la Ley de Privacidad del Consumidor de California (“CCPA”)
- La Ley General de Protección de Datos de Brasil (“LGPD”)
- Ley de Protección de la Información Personal y de los Documentos Electrónicos de Canadá (“PIPEDA”)
- Ley de Protección de Información Personal de Japón (“APPI”)

La flexibilidad y la escala de la plataforma de Elastic permiten a las organizaciones navegar y gestionar el cumplimiento de estos requisitos legales tan diversos y complejos.

Datos personales

Los días en que el concepto de “datos personales” se limitaba a identificadores obvios como nombres y apellido, direcciones de correo electrónico, identificadores gubernamentales y números de teléfono han quedado atrás. Hoy en día, las leyes de privacidad de todo el mundo definen los datos personales de forma amplia para abarcar cualquier información que pueda asociarse con un dispositivo o persona específica.

Una buena regla práctica sería suponer que las leyes de privacidad probablemente se aplican si la información puede vincularse a un identificador único de una persona. Con smartphones, dispositivos IoT y otros dispositivos informáticos omnipresentes en la vida cotidiana, la recopilación de datos personales aumentó en organizaciones de todos los sectores, creando una necesidad urgente e innegable de productos y servicios que permitan a las organizaciones gestionar con confianza el procesamiento de dichos datos.

Controladores y procesadores

Las leyes de privacidad de todo el mundo típicamente imponen obligaciones diferentes, pero a menudo superpuestas, a las organizaciones dependiendo de si actúan como un "controlador" o un "procesador" de los datos personales.

- Los **controladores** (también llamados “negocios” bajo la CCPA) controlan los propósitos y los medios de procesamiento de datos personales. Son las entidades que toman decisiones independientes sobre qué datos personales recopilarán y cómo los procesarán.
- Los **procesadores** (también llamados “proveedores de servicios” según la CCPA) brindan servicios a un controlador ascendente (o, a veces, a otro procesador) y solo se les permite procesar datos personales estrictamente de acuerdo con las instrucciones del controlador con el propósito de proporcionar servicios al controlador.

Aunque se aplican diferentes obligaciones a los controladores y procesadores, el cumplimiento en cada rol requiere comprender los tipos de datos personales que se están tratando y ser capaz de localizar los datos personales de forma dirigida, escalable y eficiente.

La mayoría de las leyes de privacidad de todo el mundo también otorgan a las personas ciertos derechos sobre sus datos, como el acceso, la eliminación y la corrección. Con plazos relativamente cortos para responder, emplear una plataforma como Elastic para filtrar eficientemente sets de datos estructurados y no estructurados no solo ayudará a agilizar el cumplimiento, sino que también reducirá los riesgos de investigaciones regulatorias y litigios civiles.

Principios fundamentales de privacidad.

Las leyes globales de privacidad a menudo se basan en principios fundamentales de privacidad. En general, estos son:

1

Aviso

Las leyes de privacidad exigen que las organizaciones proporcionen información precisa y actualizada sobre sus prácticas de privacidad.

2

Privacidad por diseño

Las leyes de privacidad exigen que las organizaciones reflexionen sobre cómo sus prácticas pueden afectar los derechos de privacidad y los intereses de las personas, y diseñen sus productos para cumplir con esas leyes.

3

Derechos

Las leyes de privacidad otorgan a las personas ciertos derechos sobre sus datos personales, que pueden incluir el derecho a acceder, eliminar y corregir sus datos.

4

Minimización de datos

Las leyes de privacidad exigen a las organizaciones que practiquen la minimización de datos (es decir, recopilen y procesen únicamente los datos personales necesarios para los fines empresariales para los que fueron recopilados) e impongan límites de retención y políticas de eliminación para garantizar que las organizaciones no conserven lo que no necesitan.

5

Seguridad

Las leyes de privacidad exigen ciertos estándares de seguridad para proteger los datos personales.

6

Notificación de filtraciones

Las leyes de privacidad y seguridad imponen una serie de obligaciones a las organizaciones que sufren un incidente de seguridad o una filtración de datos que afecte a datos personales.

El costo del incumplimiento

El incumplimiento de las leyes de privacidad puede conllevar sanciones severas, honorarios legales y daños para la reputación. Las sanciones regulatorias bajo marcos de trabajo como el RGPD y la CCPA pueden ser lo suficientemente grandes como para afectar materialmente los resultados de una compañía, mientras que litigantes civiles también pueden presentar reclamaciones por violaciones de privacidad, incluyendo demandas colectivas después de filtraciones de datos.

Según un reporte de IBM Security y el Ponemon Institute, el costo promedio de una filtración de datos en 2024 fue de 4.88 millones de dólares, lo que supuso un aumento del 10 % o con respecto al año anterior. El reporte sobre riesgos cibernéticos de AON reveló que 56 incidentes cibernéticos muy publicitados causaron pérdidas en el precio de las acciones del 27 % para las organizaciones afectadas en promedio en 2024. Es evidente que este tipo de daño a la reputación también puede afectar de manera irreversible a la ventaja competitiva de una organización. En este contexto, el cumplimiento normativo no es solo un gasto, sino una inversión estratégica.

Uso de Elastic para tus necesidades de cumplimiento de las reglamentaciones de protección de datos

Elastic ayuda a las organizaciones a encontrar respuestas relevantes que importan a una velocidad sin precedentes con soluciones empresariales abiertas y flexibles. El cumplimiento de las leyes de privacidad en todo el mundo requiere una comprensión de todo tu ecosistema de datos: dónde residen los datos personales, cómo se mueven y cómo se procesan esos datos. Aquí es donde la Elasticsearch Platform destaca, simplificando y automatizando estos procesos para lograr un cumplimiento sin complicaciones. A continuación, describimos el valor de Elastic en relación con los seis principios fundamentales de privacidad explicados anteriormente.

Aviso

Las características de mapeo de datos de Elastic permiten a las organizaciones comprender el alcance y los tipos de datos personales en todos los servidores de una organización y más allá.

La notificación es un principio fundacional del núcleo de las leyes de privacidad. Las personas tienen derecho a comprender los tipos de datos personales que una organización recopila sobre ellas, los fines de la recopilación y las circunstancias en las que sus datos se divulgan a terceros. Las leyes de privacidad de datos suelen exigir a las organizaciones que proporcionen políticas de privacidad completas, como la Declaración de Privacidad de Elastic, que explica estos conceptos, como se hace en el Centro de Confianza de Elastic.

Para cumplir con este principio de notificación, una organización debe comprender el alcance de los datos personales que recopila. Esto requiere un ejercicio estable de mapeo de datos, que es un proceso sistemático que identifica y documenta todos los flujos de datos personales dentro de una organización.

Sin una solución escalable, las organizaciones a menudo se ven obligadas a depender de una acumulación de hojas de cálculo anticuadas, respuestas a encuestas de inventario de datos y entrevistas improvisadas con diversas unidades de negocio para identificar los datos personales recogidos y cómo se trasladan dentro y fuera de la organización.

En el mejor de los casos, los registros pueden ser precisos en un momento dado, solo para verse afectados por las demandas de la recopilación y el procesamiento de datos en una economía impulsada por datos.

Elastic puede ayudar a las organizaciones a obtener información crucial para mejorar sus procesos de mapeo de datos. Sin conocimiento de los tipos de datos personales recopilados, dónde se encuentran dichos datos y a quién se divulgan, una organización no puede confirmar el cumplimiento de las leyes de privacidad. Al indexar la información sobre tus flujos de datos en Elastic, sus potentes capacidades de búsqueda de texto completa permiten identificar rápidamente las aplicaciones, tablas, consultas o reportes que usan datos personales.

El uso de Elastic para agilizar el mapping de datos también permite a las organizaciones cumplir con las obligaciones contractuales de las leyes de privacidad, ya que los flujos de datos identificados determinarán otras partes con las que una organización debe celebrar un anexo de protección de datos, mecanismos de transferencia de datos u otros acuerdos específicos para la protección de datos personales. Del mismo modo, las cadenas de suministro actuales pueden extenderse a cientos o miles de proveedores y subprocesadores. La capacidad de indexar y efectuar búsquedas de texto completo instantáneamente en miles de acuerdos también puede facilitar los reportes de estado de los proveedores y, lo que es más importante, permitir programas proactivos de gestión de proveedores.

Privacidad por diseño

Las organizaciones pueden utilizar Elastic para mejorar la privacidad desde el diseño, incluyendo la incorporación de principios de minimización de datos.

Si una organización está considerando usar Elastic como almacén de datos para datos personales, las capacidades de Elastic Cloud Enterprise (“ECE”), el software de orquestación central de Elastic, pueden poner a la organización en el camino correcto desde el principio. El principio de protección de datos desde su diseño consiste en tratar los datos personales como un activo valioso, limitando el acceso, manteniendo la precisión, implementando controles de seguridad de datos adecuados y limitando los periodos de retención.

A diferencia de las arquitecturas de datos tradicionales con un almacén de datos masivo y volúmenes de controles de acceso a datos complejos y superpuestos (requeridos para permitir el acceso solo a ciertos datos por varios proyectos), Elastic permite a los usuarios instanciar nuevos clústeres de Elasticsearch para cada proyecto e incluir solo los datos relevantes para ese proyecto en su clúster.

Esta arquitectura distribuida permite minimizar los datos personales, otro principio fundamental de la privacidad. Por ejemplo, los clientes pueden usar Elastic para categorizar los datos en niveles de almacenamiento, donde la información de los logs de acceso impulsada por Elastic puede ayudar a las compañías a identificar datos no empleados para informar políticas y prácticas de retención de datos.

Elastic también permite a las organizaciones comprender cuándo y cómo llevar a cabo evaluaciones de impacto sobre la privacidad de los datos (DPIA, por sus siglas en inglés). Según el RGPD y otras normativas de privacidad similares, una DPIA es una evaluación, en ocasiones obligatoria, que se utiliza para garantizar que procesas los datos personales de forma responsable y minimizas cualquier daño potencial a las personas. Saber dónde residen los datos, cómo se procesan y hacia dónde fluyen agiliza la finalización de DPIA, que tradicionalmente pueden requerir soporte multifuncional entre unidades de negocio para entender el uso de los datos personales. Las DPIA, a su vez, demuestran un cumplimiento fundamental al tiempo que permiten a las organizaciones limitar el procesamiento de datos personales a lo autorizado por las leyes globales de privacidad.

Derechos del sujeto de datos

Las organizaciones pueden utilizar Elastic para identificar datos personales relevantes, evaluar la aplicabilidad de los derechos de los interesados y atender sus solicitudes.

Las leyes de privacidad globales dan a las personas ciertas opciones sobre cómo se procesan sus datos personales. Estos suelen incluir derechos para acceder, eliminar y corregir datos personales, junto con derechos para objetar ciertos tipos de tratamiento de datos personales. Las capacidades de mapping de datos de Elastic forman el núcleo de la base por la cual las organizaciones pueden procesar las solicitudes de los sujetos de datos.

- **Acceso:** Elasticsearch permite a las organizaciones buscar en almacenes de datos para identificar datos personales en toda la organización, incluida la identificación de tablas, consultas, reportes o aplicaciones que dependen de datos personales. Las organizaciones pueden también aprovechar Elastic para potenciar las funciones de búsqueda del usuario final, de modo que los usuarios finales pueden buscar sus datos de usuario. Otorgar a los usuarios finales potentes capacidades de búsqueda reduce las demandas de Atención al cliente, ya que los usuarios finales pueden usar herramientas de autoservicio para identificar y exportar sus datos. En caso de que las herramientas de autoservicio no sean suficientes, Elastic permite a las organizaciones buscar rápidamente sus propios almacenes de datos para honrar las solicitudes de acceso de las personas.

- **Eliminación:** Después de usar Elastic para identificar los datos personales mantenidos sobre una persona, una organización puede usar Elastic para transformar dichos datos, incluso etiquetar datos para su retención bajo una excepción de eliminación, eliminar datos de forma permanente y usar otras técnicas de eliminación que puedan estar permitidas según las leyes de privacidad, incluida la anonimización y ciertos tipos de seudonimización de datos personales. El uso de Elastic para transformar los datos personales rápidamente y sin una costosa estructura de ingeniería ayuda a las organizaciones a cumplir con las normas, evitar el escrutinio regulatorio y mantener la utilidad de los datos dentro de los límites de las leyes de privacidad de todo el mundo.

- **Corrección:** Del mismo modo, las leyes de privacidad suelen permitir que las personas soliciten la corrección de sus datos personales. Elastic puede aislar los datos personales mantenidos sobre una persona para que la organización pueda centrarse en procesar la solicitud, no en encontrar los datos.

- **Restricciones:** Algunas leyes de privacidad, como el RGPD y su equivalente en el Reino Unido, también incluyen el derecho a objetar o a aplicar el tratamiento restringido de datos personales. Las organizaciones pueden emplear las capacidades de mapping y categorización de datos de Elastic para determinar rápidamente cómo responder a estas solicitudes y restringir las licencias de acceso y uso en consecuencia, ahorrando un tiempo valioso para que los equipos de cumplimiento respondan en los plazos cortos que permiten estas leyes.

Minimización de datos

Como se anticipó en la *sección Privacidad por diseño*, Elastic potencia las capacidades de minimización de datos para empresas. Los principios de minimización de datos exigen que las organizaciones recopilen, procesen y limiten la retención de datos personales a la información necesaria para lograr los fines autorizados de procesamiento.

Por ejemplo, una forma de minimizar el procesamiento de datos personales para cumplir con esta obligación es mediante **la seudonimización** (es decir, sustituir los identificadores personales en los datos por valores de marcador de posición) o **la anonimización** (es decir, eliminar por completo los identificadores personales de los datos para que ya no sea posible identificar a una persona). Conoce cómo una aerolínea europea líder utiliza el pipeline de ingesta de Elastic para ocultar los datos confidenciales antes de su almacenamiento. Estos resultados se pueden lograr utilizando Logstash, una integración disponible en Elastic que ingiere datos de múltiples fuentes para facilitar la transformación de dichos datos, incluyendo la anonimización y la seudonimización, lo que permite avanzar en los objetivos de minimización de datos y reducir los riesgos de seguridad.

El uso de Elastic para el mapeo y la auditoría de datos también permite a las organizaciones analizar más de cerca su uso real de los datos personales retenidos, lo que permite a la organización adaptar de manera más efectiva los períodos y políticas de retención de datos.

Seguridad y notificación de filtraciones

Para obtener más información sobre cómo Elastic puede ayudar a las organizaciones a proteger sus datos personales y responder rápidamente en caso de una filtración de datos, consulta nuestro Reporte técnico de seguridad.

Conclusión

La privacidad de datos no es solo un requisito regulatorio; es un imperativo comercial. Con multas elevadas, interrupciones empresariales, daños reputacionales y la confianza del cliente en juego, las organizaciones necesitan una forma fiable y escalable de mapear, categorizar, gestionar, transformar, analizar y eliminar sus datos. Elastic optimiza cada paso de este proceso, proporcionando la potencia escalable que tu organización necesita para garantizar el cumplimiento normativo y la confianza de los clientes.

