Evaluación del impacto de las transferencias de Elastic

Australia

Los clientes son responsables de realizar su propia evaluación independiente de la información en este documento. Este documento: (a) tiene fines meramente informativos, (b) representa las ofertas de productos, servicios y prácticas actuales de Elastic, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de Elastic y sus afiliadas, proveedores o licenciantes. Las responsabilidades y obligaciones de Elastic frente a sus clientes se rigen por los acuerdos de Elastic, y este documento no forma parte ni modifica ningún acuerdo entre Elastic y sus clientes.

Última revisión: octubre de 2025

Introducción a las transferencias de datos de Elastic y Marco de trabajo de evaluación

Las ofertas de Elastic

Elastic proporciona un conjunto de productos de Elasticsearch, Observability y Security y características asociadas, que están diseñados para brindar a los clientes información en tiempo real y robustas capacidades de gestión de datos.

Elastic puede tratar datos personales por cuenta de nuestros clientes en calidad de encargado del tratamiento ("Datos personales del cliente") cuando los clientes implementan productos y funciones de Elastic en Elastic Cloud, o cuando utilizan los Servicios de soporte o los Servicios de consultoría de Elastic (las "Ofertas de Elastic"), cada uno con alcances específicos de tratamiento de datos personales.

Elastic Cloud ofrece una plataforma alojada para que los clientes puedan implementar las soluciones de búsqueda, observabilidad y seguridad de Elastic en Amazon Web Services, Microsoft Azure y Google Cloud. Puedes elegir tu región de alojamiento de datos preferida entre muchas opciones globales, incluidas numerosas ubicaciones dentro del Espacio Económico Europeo (EEE). De forma predeterminada, los backups se almacenan en la misma región que tu despliegue. Si bien controlas la residencia de tus datos, el personal y los subprocesadores de Elastic pueden requerir acceso limitado a datos desde fuera del EEE para servicios esenciales como la gestión de la plataforma, las operaciones técnicas y la atención al cliente.

Los Servicios de soporte ofrecen asistencia integral a los usuarios de productos Elastic, que abarcan desde la ingesta inicial de datos hasta el escalado de los despliegues y la obtención de información valiosa. En el contexto de los datos personales de los clientes, las actividades de procesamiento de Elastic durante los compromisos de soporte están altamente restringidas. Los agentes de soporte interactúan principalmente con la capa administrativa de Elastic Cloud, lo que minimiza el acceso directo al contenido de los datos de los clientes almacenados en los índices. Si un problema excepcional requiere que un agente de soporte acceda directamente al contenido del cliente o a los índices de datos del cliente, que pueden incluir datos personales implicados (por ejemplo, para analizar un volcado de memoria), la aprobación del cliente es un requisito obligatorio. Estos procesos están sujetos a controles estrictos, auditabilidad y adherencia a estándares de cumplimiento reconocidos.

Los Servicios de consultoría ofrecen orientación basada en resultados para ayudar a las organizaciones a optimizar el uso de Elastic Stack, agilizar los plazos de los proyectos y alcanzar objetivos empresariales específicos. Estos servicios se proporcionan globalmente con opciones de entrega flexibles y virtuales. De manera similar al soporte, la prestación de servicios de consultoría puede implicar el procesamiento de los datos personales del cliente según sea necesario para ayudar en la prestación del servicio de consultoría acordado.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

Procesamiento de datos personales de Elastic

Al proporcionar servicios a sus clientes, Elastic actúa como encargado del tratamiento de los datos. La naturaleza definitiva y las categorías de los Datos personales del cliente procesados se determinan y controlan por los clientes de Elastic a su entera discreción. Elastic no supervisa de forma activa los datos específicos que los clientes ingestan en sus servicios.

La siguiente tabla resume el tratamiento de los datos personales de los clientes para cada una de las ofertas de Elastic:

Oferta de Elastic	*Propósito de procesamiento primario*	*Naturaleza de los datos personales procesados*	*Categorías de datos*	*Control de ubicación de alojamiento / procesamiento*
Elastic Cloud	Información en tiempo real, búsqueda, observabilidad, analítica de seguridad, gestión de plataformas, operaciones técnicas	Datos personales del cliente (contenido determinado por el cliente, no supervisado por Elastic), datos operativos limitados (por ejemplo, registros de uso, identificadores en línea, comunicaciones electrónicas, datos de actividad de red) para la gestión de la plataforma.	Administradores de clientes, usuarios finales, personal de los clientes y socios del cliente	El cliente selecciona su región preferida para el alojamiento de datos (hay opciones disponibles en el EEE), los backups se realizan en la misma región. Determinadas actividades de procesamiento (gestión de la plataforma, operaciones técnicas, soporte) pueden implicar un acceso limitado desde fuera del EEE.
Servicios de soporte	Asistencia integral, resolución de problemas y orientación técnica	Acceso a los datos personales del cliente muy limitado (principalmente interacción a nivel de la capa administrativa). Acceso directo al contenido del cliente (por ejemplo, volcado de memoria) solo con la aprobación del cliente.	Administradores de clientes, usuarios finales	Esto puede implicar que Elastic y los subprocesadores accedan a la información desde lugares fuera del EEE.
Servicios de consultoría	Consultoría basada en resultados, optimización de proyectos, resultados de negocio con Elastic Stack	Datos personales del cliente, en la medida en que sean necesarios para facilitar la prestación del servicio.	Administradores de clientes, usuarios finales	Esto puede implicar que Elastic y los subprocesadores accedan a la información desde lugares fuera del EEE.

Base legal para transferencias internacionales: cláusulas contractuales estándar (SCC)

El marco de trabajo de Elastic para las transferencias internacionales de datos se basa firmemente en el uso de cláusulas contractuales estándar (SCC). Este mecanismo se utiliza tanto para transferencias directas, en las que los datos fluyen del cliente a Elastic, como para transferencias posteriores, de Elastic a sus subprocesadores internos y subprocesadores externos, con el fin de alinearse directamente con los requisitos establecidos por el Tribunal de Justicia de la Unión Europea (TJUE) en su sentencia “Schrems II”. La decisión “Schrems II”, emitida el 16 de julio de 2020, invalidó el Escudo de Privacidad UE-EE. UU., pero al mismo tiempo reafirmó la validez de las Cláusulas contractuales estándar (SCC) como una herramienta legítima para la transferencia de datos personales desde el Espacio Económico Europeo (EEE) a terceros países. Sin embargo, la sentencia del TJUE también estableció que los importadores y exportadores de datos deben realizar una evaluación detallada, caso por caso, de la transferencia e implementar salvaguardas adicionales cuando sea necesario, para garantizar que los datos personales mantengan un nivel de protección “esencialmente equivalente” al garantizado dentro del EEE.

Esta evaluación ofrece una revisión exhaustiva de los aspectos legales y prácticos relacionados con las transferencias de datos al país correspondiente que se enumeran a continuación. Analizamos la legislación de acceso gubernamental relevante, evaluamos la efectividad de las SCC y detallamos las medidas específicas de Elastic para mitigar los riesgos.

Evaluación del impacto de transferencias en Australia

Esta sección ofrece una evaluación detallada del panorama legal y práctico de las transferencias de datos a Australia, y analiza la legislación aplicable sobre acceso gubernamental, la eficacia de las SCC y las medidas específicas de mitigación implementadas por Elastic.

Legislación aplicable sobre acceso gubernamental y alcance de la vigilancia

El marco de trabajo legal de Australia permite a las autoridades gubernamentales acceder a datos personales para vigilancia, inteligencia, seguridad nacional y aplicación de la ley penal, al tiempo que mantiene por lo general condiciones estrictas.

- **Ley de Privacidad de 1988 (Cth) ("Ley de Privacidad"):** esta ley exige el cumplimiento de los Principios de Privacidad de Australia (APP), que generalmente restringen la recopilación, el uso y la divulgación encubiertos de información personal por parte de autoridades públicas. Sin embargo, incluye excepciones explícitas para las actividades de aplicación de la ley donde el uso o la divulgación de datos es "razonablemente necesario". La ley también incluye requisitos obligatorios de notificación de brechas de datos.

- **Ley de Dispositivos de Vigilancia de 2004 (Cth) ("SDA"):** la SDA faculta a las agencias federales de aplicación de la ley para obtener órdenes judiciales de jueces o magistrados autorizados para la instalación y el uso de dispositivos de vigilancia y el acceso a datos informáticos. Está prohibida la vigilancia encubierta sin orden judicial.

- **Ley de Telecomunicaciones de 1997 (Cth) ("TA"):** esta ley permite que determinadas agencias de aplicación de la ley obliguen a organizaciones privadas a prestar asistencia, incluido el acceso a sistemas de comunicación y la ruptura de cifrado, sin requerir una orden judicial. Existe un mecanismo de supervisión, como el Inspector General de Inteligencia y Seguridad, para atender denuncias relacionadas con solicitudes irrazonables.

- **Ley de Telecomunicaciones (Intercepción y Acceso) de 1979 (Cth) ("TIA"):** la TIA permite a las fuerzas de seguridad acceder a comunicaciones transmitidas o almacenadas mediante una orden judicial, que puede obtenerse por razones de seguridad nacional (a través del Fiscal General o del Director General de Seguridad) o por delitos penales graves (a través de un juez). La TIA también exige que los "proveedores de servicios de transporte" (CSP) conserven un subconjunto definido de metadatos de telecomunicaciones durante dos años y proporcionen acceso a ellos mediante una orden judicial.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

- **Alcance del importador de datos:** Elastic procesa los datos personales de clientes B2B, que pueden estar hospedados en servidores en Australia, por lo que están sujetos a estos poderes gubernamentales.[1] Elastic afirma que la TA y la TIA requieren específicamente que las organizaciones privadas cooperen con las autoridades competentes cuando sea necesario para el cumplimiento de la ley o la seguridad nacional.

Evaluación de la eficacia de la herramienta de transferencia y desafíos legales

La efectividad de las SCC en Australia es generalmente fuerte debido a un sólido marco de privacidad, pero las disposiciones legislativas específicas presentan desafíos.

Un desafío clave proviene de la Ley de Telecomunicaciones (TA), que permite a ciertas agencias exigir asistencia, incluido romper el cifrado, sin una orden judicial. Aunque existe un organismo de supervisión, esta coerción directa sin revisión judicial previa plantea preocupaciones con respecto a los principios de necesidad y proporcionalidad del GDPR. Además, la retención obligatoria de metadatos de telecomunicaciones durante dos años bajo el TIA, incluso si no es contenido, representa una forma de recopilación masiva de datos que justifica el escrutinio bajo los principios de minimización de datos y proporcionalidad del GDPR.

A pesar de estos desafíos específicos, el sistema legal de Australia generalmente impone condiciones estrictas al acceso del gobierno a la información personal, lo que a menudo requiere órdenes judiciales. La Ley de Privacidad, junto con sus Principios de Privacidad de Australia (APP), es una ley integral supervisada y aplicada por el Comisionado de Privacidad, una figura independiente que forma parte de la Oficina del Comisionado de Información de Australia (OAIC). La OAIC maneja quejas y puede iniciar investigaciones. Además, el Defensor del Pueblo de la Commonwealth inspecciona los registros de las agencias de aplicación de la ley para verificar el cumplimiento de la TIA. El marco de Australia se alinea con las Prácticas Justas de Información (FIPP) de la OCDE, lo que garantiza principios como la limitación de la finalidad, la seguridad de los datos y la notificación al individuo.

El marco de trabajo de Australia se caracteriza por una ley de privacidad sólida y completa (Ley de Privacidad con APP) y un regulador independiente (OAIC). Sin embargo, leyes específicas de seguridad nacional y aplicación de la ley (TA, TIA) otorgan poderes para la asistencia obligatoria y la retención de metadatos que no siempre se ajustan a la estricta necesidad y proporcionalidad del GDPR, especialmente cuando no siempre se requieren órdenes judiciales para ciertos tipos de acceso o asistencia. Aunque el sistema jurídico en general parece sólido, la existencia de estos poderes específicos y potencialmente amplios implica que una TIA no puede limitarse a basarse en el marco de trabajo general de protección de la privacidad.

Dicho esto, Elastic no es un “operador” de telecomunicaciones en el sentido de la TA y la TIA, y el propósito principal de los servicios en el cloud de Elastic no es facilitar comunicaciones electrónicas, por lo que también es poco probable que califique como un “proveedor de servicios de telecomunicaciones” dentro del alcance de dichas leyes. Como resultado, el riesgo de que se obligue a Elastic a divulgar datos de clientes en virtud de la TA o la TIA es muy bajo. Además, el compromiso de Elastic de impugnar las solicitudes y sus esfuerzos de minimización de datos constituyen medidas complementarias fundamentales para mitigar cualquier riesgo residual derivado de estas disposiciones legislativas específicas.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

Medidas específicas de Elastic para proteger y mitigar los riesgos relacionados con la protección de datos

El compromiso de Elastic con la privacidad y la seguridad de los datos se sustenta en un conjunto completo y escalonado de medidas de protección técnicas, organizativas y contractuales. Estas medidas están diseñadas para proteger los datos personales a lo largo de todo su ciclo de vida dentro de las ofertas de Elastic y para garantizar el cumplimiento de los principios de las SCC, en conformidad con el GDPR, el GDPR del Reino Unido y la Ley Federal de Protección de Datos de Suiza (FDPA).

Salvaguardas técnicas:

- **Residencia de datos:** Elastic Cloud ofrece a los clientes la flexibilidad de seleccionar su región de alojamiento de datos preferida entre una amplia gama de opciones globales en AWS, GCP y Azure, incluidas numerosas ubicaciones dentro del EEE. Esto permite a los clientes cumplir con requisitos específicos de residencia de datos, ya que los backups se almacenan automáticamente en la región elegida.
- **Cifrado en tránsito y en reposo:** los datos del cliente se cifran tanto en tránsito, utilizando TLS 1.2, como en reposo, con un mínimo de cifrados AES de 256 bits. Elastic también mantiene procedimientos sólidos de gestión de claves de cifrado.
- **Actualizaciones y parches regulares del sistema:** para minimizar los riesgos de vulnerabilidad, las instancias de Elasticsearch se despliegan en función de los núcleos del sistema operativo más recientes, con la aplicación continua de parches para abordar vulnerabilidades y exposiciones comunes (CVE).
- **Uso de proveedores de servicios líderes en la industria:** Los servicios de Elastic están alojados en centros de datos gestionados por grandes proveedores de servicios en la cloud, reconocidos por sus medidas de seguridad técnicas y organizacionales de última generación diseñadas para proteger los datos alojados.
- **Controles de acceso:** Elastic aplica controles lógicos y administrativos estrictos para limitar el acceso a los datos exclusivamente a los usuarios autorizados. Esto incluye autenticación multifactor, estándares de contraseña sólidos y el uso de VPN para el acceso administrativo. El principio de privilegio mínimo se cumple estrictamente, lo que garantiza que los empleados solo tengan el acceso necesario para sus funciones, con revisiones regulares de los derechos de acceso. El logging centralizado, que incluye los logs de proxy, de acceso, de Elasticsearch y de Auditbeat, registra minuciosamente todos los accesos a los datos de los clientes y a los sistemas donde se almacenan. Para los servicios de soporte, el acceso a los Datos personales del cliente es muy limitado, y los agentes interactúan principalmente con la capa administrativa y requieren autorización del cliente para acceder al contenido.
- **Detección y respuesta de incidentes:** Elastic mantiene y actualiza continuamente reglas sofisticadas de detección para actividad sospechosa y acceso no autorizado, lo que incluye monitoreo de integridad de archivos e indicadores de apropiación de cuenta. Estas detecciones se integran en flujos de trabajo automatizados que alertan al equipo de Detección y Respuesta a Amenazas, y desencadenan investigaciones inmediatas.

Medidas de seguridad organizativas:

- **Sistema de gestión de seguridad de la información (ISMS):** Elastic adoptó formalmente un ISMS certificado de conformidad con las normas ISO 27001, ISO 27017 y ISO 27018. Este sistema constituye la base de todas las políticas, normas y directrices de seguridad de la información, y garantiza medidas técnicas y organizativas integrales para la protección de datos.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

- **Privacidad y seguridad por diseño:** estos principios están integrados en cada producto Elastic desde su concepción hasta su despliegue, lo que garantiza que la protección de datos sea un aspecto fundamental del desarrollo del producto.
- **Principios para las solicitudes de información de las autoridades públicas:** Elastic estableció principios y procedimientos claros para gestionar las solicitudes de información de clientes por parte de las autoridades públicas. Estos protocolos incluyen impugnar solicitudes, notificar a las partes relevantes y solicitar exenciones de las prohibiciones de notificación. Elastic nunca creó puertas traseras ni claves maestras para sus productos y nunca permitió que ninguna autoridad gubernamental tenga acceso irrestricto o directo a sus servidores.
- **Gestión de la cadena de suministros:** Elastic lleva a cabo un proceso exhaustivo de debida diligencia interfuncional que involucra a los equipos de seguridad, privacidad y cumplimiento para todos los proveedores de servicios. Esto incluye revisar el tipo y el nivel de riesgo de los datos que se van a compartir, las políticas y medidas de seguridad del proveedor, las auditorías de terceros y realizar evaluaciones de impacto en la privacidad.
- **Otras políticas internas:** Elastic mantiene políticas internas que regulan el uso y acceso a datos personales, la gestión de brechas de datos, las solicitudes de acceso de los interesados, la retención de datos y el control de acceso.
- **Marcos de cumplimiento:** Elastic Cloud demuestra el cumplimiento con una amplia gama de marcos de la industria, incluidos SOC 2 Tipo II, CSA CCM 4.0, PCI-DSS, HIPAA, Cyber Essentials+, la Directiva NIS2 para proveedores de servicios en el cloud, TISAX y FedRAMP Moderado.
- **Pruebas regulares:** se realizan pruebas periódicas de vulnerabilidad y penetración de la red y las aplicaciones, con procedimientos establecidos para documentar y abordar cualquier vulnerabilidad descubierta.
- **Capacitación de empleados:** todos los empleados deben completar la capacitación en seguridad de la información, protección de datos y privacidad al momento de su contratación y, posteriormente, de forma anual.

Salvaguardias contractuales:

- **Anexo de procesamiento de datos (DPA):** Elastic se compromete contractualmente a aplicar sólidas medidas de protección de datos y privacidad en virtud de nuestro Anexo de protección de datos, que incluye las SCC y sus variantes para Suiza y el Reino Unido, así como nuestro Anexo de seguridad de la información. Revisamos y actualizamos regularmente nuestro Anexo de procesamiento de datos para que refleje los requisitos de privacidad de datos aplicables y las mejores prácticas.
- **Instrucciones para el cliente:** el procesamiento de los datos personales del cliente se realiza estrictamente siguiendo solo las instrucciones del cliente.
- **Confidencialidad:** todo el personal autorizado para procesar los datos personales del cliente está sujeto a estrictos acuerdos, políticas y procedimientos de confidencialidad.
- **Control:** los clientes mantienen la capacidad de recuperar, corregir o eliminar cualquier dato personal que suban a Elastic Cloud en cualquier momento.
- **Notificación de solicitudes de divulgación:** Elastic se compromete contractualmente a notificar a los clientes en caso de recibir una solicitud de divulgación de sus datos, salvo que la ley prohíba hacerlo.
- **Obligaciones de los subprocesadores:** somos totalmente transparentes respecto a nuestros subprocesadores, que también están sujetos a los mismos estrictos estándares y requisitos organizacionales. Somos responsables de los actos y las omisiones de nuestros subprocesadores en la misma medida que si prestáramos los servicios nosotros mismos.

© 2025 Elasticsearch B.V. Todos los derechos reservados.