Elastic Transfer Impact Assessment

Australia

Last Revision: October 2025

Introduction to Elastic's Data Transfers and Assessment Framework

The Elastic Offerings

Elastic provides a suite of Elasticsearch, Observability, and Security products and associated features designed to empower customers with real-time insights and robust data management capabilities.

Elastic may process personal data on behalf of our customers as a processor ("Customer Personal Data") when customers deploy Elastic products and features in Elastic Cloud, or when customers utilize Elastic's Support Services, and/or Consulting Services (the "Elastic Offerings"), each with distinct scopes of personal data processing.

Elastic Cloud provides a hosted platform for customers to deploy Elastic's Search, Observability, and Security solutions across Amazon Web Services, Microsoft Azure, and Google Cloud. You can choose your preferred data hosting region from many global options, including numerous locations within the European Economic Area (EEA). By default, backups are stored in the same region as your deployment. While you control your data residency, Elastic personnel and sub-processors may require limited data access from outside the EEA for essential services like platform management, technical operations, and customer support.

Support Services offer comprehensive assistance to Elastic product users, covering everything from initial data ingestion to scaling deployments and deriving meaningful insights. In the context of Customer Personal Data, Elastic's processing activities during support engagements are highly restricted. Support agents primarily interact with the administrative layer of Elastic Cloud, minimizing direct access to the content of customer data stored in indices. Should an exceptional issue require a support agent to directly access customer content or customer data indices, which may include implicated personal data (e.g., for analyzing a heap dump), approval from the customer is a mandatory prerequisite. These processes are subject to strict controls, auditability, and adherence to recognized compliance standards.

Consulting Services deliver outcome-based guidance to help organizations optimize their use of the Elastic Stack, streamline project timelines, and achieve specific business objectives. These services are provided globally with flexible virtual delivery options. Similar to support, the provision of consulting services may involve processing Customer Personal Data as necessary to assist in the agreed-upon consulting service delivery.

Elastic's Personal Data Processing

In provisioning services to its customers, Elastic acts as a data processor. The ultimate nature and categories of Customer Personal Data processed are determined and controlled by Elastic's customers in their sole discretion. Elastic does not actively monitor the specific data that customers ingest into its offerings.

The following table summarizes Customer Personal Data processing for each of the Elastic Offerings:

Elastic Offering	Primary Processing Purpose	Nature of Personal Data Processed	Categories of Data Subjects	Hosting / Processing Location Control
Elastic Cloud	Real-time insights, search, observability, security, analytics, platform management, technical operations	Customer Personal Data (content determined by customer, not monitored by Elastic), limited operational data (e.g., usage logs, online identifiers, electronic communication, network activity data) for platform management.	Customer admins, end-users, customer's clients/partners' workforce	Customer selects preferred data hosting region (EEA options available), backups in the same region. Certain processing activities (platform management, tech ops, support) may involve limited access from outside EEA.
Support Services	Comprehensive assistance, troubleshooting, technical guidance	Highly limited Customer Personal Data access (primarily administrative layer interaction). Direct access to customer content (e.g., heap dump) only with customer approval.	Customer admins, end-users	May involve Elastic and sub-processors access from locations outside EEA.
Consulting Services	Outcome-based consulting, project streamlining, business outcomes with Elastic Stack	Customer Personal Data as necessary to assist in service provision.	Customer admins, end-users	May involve Elastic and sub-processors access from locations outside EEA.

Legal Basis for International Transfers: Standard Contractual Clauses (SCCs)

Elastic's framework for international data transfers is firmly rooted in the use of the Standard Contractual Clauses (SCCs). This mechanism is employed for both direct transfers, where data flows from the customer to Elastic, and for onward transfers, from Elastic to its internal and external sub-processors, to align directly with the requirements set forth by the Court of Justice of the European Union (CJEU) in its "Schrems II" ruling. The "Schrems II" decision, issued on July 16, 2020, invalidated the EU-US Privacy Shield but simultaneously reaffirmed the validity of SCCs as a legitimate transfer tool for personal data from the European Economic Area (EEA) to third countries. However, the CJEU's ruling also mandated that data importers and exporters conduct a detailed, case-by-case assessment of the transfer and implement additional safeguards where necessary, to ensure that personal data maintains a level of protection "essentially equivalent" to that guaranteed within the EEA.

This assessment offers a comprehensive review of the legal and practical aspects surrounding data transfers to the applicable country listed below. We've analyzed the relevant government access legislation, evaluated the effectiveness of the SCCs, and detailed Elastic's specific measures for mitigating risks.

Australia Transfer Impact Assessment

This section provides a detailed assessment of the legal and practical landscape for data transfers to Australia, analyzing applicable government access legislation, the effectiveness of the SCCs, and Elastic's specific mitigating measures.

Applicable Government Access Legislation and Surveillance Scope

Australia's legal framework permits government authorities to access personal data for surveillance, intelligence, national security, and criminal law enforcement, while generally maintaining strict conditions.

- **Privacy Act 1988 (Cth) ("Privacy Act"):** This Act mandates compliance with the Australian Privacy Principles (APPs), which generally restrict covert collection, use, and disclosure of personal information by public authorities. However, it includes explicit exceptions for law enforcement activities where data use or disclosure is "reasonably necessary". The Act also includes mandatory data breach notification requirements.

- **Surveillance Devices Act 2004 (Cth) ("SDA"):** The SDA empowers Federal law enforcement agencies to obtain warrants from eligible judges or magistrates for the installation and use of surveillance devices and access to computer data. Covert surveillance without a warrant is prohibited.

- **Telecommunications Act 1997 (Cth) ("TA"):** This Act allows specified law enforcement agencies to compel assistance from private organizations, including access to communication systems and the breaking of encryption, without requiring a warrant. An oversight mechanism, such as the Inspector-General of Intelligence and Security, exists for complaints regarding unreasonable requests.

- **Telecommunications (Interception & Access) Act 1979 (Cth) ("TIA"):** The TIA permits law enforcement access to transmitted or stored communications under a warrant, which can be obtained for national security reasons (from the Attorney General or Director-General of Security) or for serious criminal offenses (from a judge). The TIA also mandates 'Carriage Service Providers' (CSPs) to retain a defined subset of telecommunications metadata for two years and provide access under a warrant.

- **Data Importer's Scope:** Elastic processes B2B Customer Personal Data, which may be hosted on servers in Australia, making it subject to these governmental powers.[1] Elastic states that the TA and TIA specifically require private organizations to cooperate with law enforcement agencies when necessary for law enforcement or national security.

Assessment of Effectiveness of Transfer Tool & Legal Challenges

The effectiveness of SCCs in Australia is generally strong due to a robust privacy framework, but specific legislative provisions present challenges.

A key challenge stems from the Telecommunications Act (TA), which allows certain agencies to compel assistance, including breaking encryption, without a warrant. While an oversight body exists, this direct compulsion without prior judicial review raises concerns regarding GDPR's necessity and proportionality

principles. Additionally, the mandatory retention of telecommunications metadata for two years under the TIA , even if not content, represents a form of mass data collection that warrants scrutiny under GDPR's data minimization and proportionality principles.

Despite these specific challenges, Australia's legal system generally imposes strict conditions on government access to personal information, often requiring warrants. The Privacy Act, with its Australian Privacy Principles (APPs), is a comprehensive law overseen and enforced by the independent Privacy Commissioner (part of the Office of the Australian Information Commissioner - OAIC). The OAIC handles complaints and can initiate investigations. Furthermore, the Commonwealth Ombudsman inspects enforcement agency records for TIA compliance. Australia's framework aligns with the OECD's Fair Information Practices (FIPPs), ensuring principles like purpose limitation, data security, and individual notice.

Australia's framework is characterized by a strong, comprehensive privacy law (Privacy Act with APPs) and an independent regulator (OAIC). However, specific national security and law enforcement acts (TA, TIA) carve out powers for compelled assistance and metadata retention that might not always align with the strict necessity and proportionality of GDPR, particularly when warrants are not always required for certain types of access or assistance. While the overall legal system appears robust, the existence of these specific, potentially broad powers means that a TIA cannot simply rely on the general privacy framework.

That being said, Elastic is not a telecommunications “carrier” in the meaning of the TA and TIA, and the primary purpose of Elastic’s cloud services is not to facilitate electronic communications, such that Elastic is also unlikely to qualify as a “carriage service provider” in scope of the same. As a result, the risk of Elastic being compelled to disclose customer data under the TA or TIA is very low. Furthermore, Elastic's commitment to challenging requests and its data minimization efforts are crucial supplementary measures to mitigate any residual risks posed by these specific legislative provisions.

Elastic's Specific Safeguards and Mitigating Data Protection Measures

Elastic's commitment to data privacy and security is underpinned by a comprehensive and layered set of technical, organizational, and contractual safeguards. These measures are designed to protect personal data throughout its lifecycle within Elastic Offerings and to uphold the principles of the SCCs, in compliance with GDPR, UK GDPR, and the Swiss FDPA.

Technical Safeguards:

- **Data Residency**: Elastic Cloud provides customers with the flexibility to select their preferred data hosting region from a wide array of global options across AWS, GCP, and Azure, including numerous locations within the EEA. This enables customers to meet specific data residency requirements, with backups automatically stored in the chosen region.
- **Encryption on Transfer and at Rest**: Customer data is encrypted both in transit, utilizing TLS 1.2, and at rest, employing a minimum of AES-256 bit ciphers. Elastic also maintains robust encryption key management procedures.
- **Regular System Updates and Patches**: To minimize vulnerability risks, Elasticsearch instances are deployed based on the latest operating system kernels, with continuous application of patches to address Common Vulnerabilities and Exposures (CVEs).
- **Use of Industry-Leading Service Providers**: Elastic's services are hosted on data centers managed by

major cloud service providers, which are recognized for their state-of-the-art technical and organizational security measures designed to protect hosted data.

- **Access Controls**: Elastic implements stringent logical and administrative controls to limit data access strictly to authorized users. This includes multi-factor authentication, strong password standards, and the use of VPNs for administrative access. The principle of least privilege is strictly adhered to, ensuring employees only have access necessary for their roles, with regular reviews of access rights. Centralized logging, encompassing proxy, access, Elasticsearch, and Auditbeat logs, meticulously records all access to customer data and the systems where it resides. For support services, access to Customer Personal Data is highly limited, with agents primarily interacting with the administrative layer and requiring customer authorization for access to content.
- **Incident Detection and Response**: Elastic maintains and continuously updates sophisticated detection rules for suspicious activity and unauthorized access, including file integrity monitoring and account takeover indicators. These detections are integrated into automated workflows that alert the Threat Detection and Response team, triggering immediate investigations.

Organizational Safeguards:

- **Information Security Management System (ISMS)**: Elastic has formally adopted an ISMS certified under ISO 27001, ISO 27017, and ISO 27018. This system forms the backbone of all information security policies, standards, and guidelines, ensuring comprehensive technical and organizational measures for data protection.
- **Privacy and Security by Design**: These principles are embedded into every Elastic product from its conception through to deployment, ensuring that data protection is a fundamental aspect of product development.
- **Principles for Public Authority Requests for Customer Information**: Elastic has established clear principles and procedures for managing requests for customer information from public authorities. These protocols include challenging requests, notifying relevant parties, and seeking waivers from notification prohibitions. Elastic has never created backdoors or master keys for its products and has never allowed any government authority unfettered or direct access to its servers.
- **Supply Chain Management**: Elastic conducts a thorough, cross-functional due diligence process involving security, privacy, and compliance teams for all service providers. This includes reviewing the type and risk level of data to be shared, the supplier's security policies, measures, and third-party audits, and conducting privacy impact assessments.
- **Other Internal Policies**: Elastic maintains internal policies governing the use and access to personal data, data breach management, data subject access requests, data retention, and access control.
- **Compliance Frameworks**: Elastic Cloud demonstrates compliance with a wide array of industry frameworks, including SOC 2 Type II, CSA CCM 4.0, PCI-DSS, HIPAA, Cyber Essentials+, NIS2 Directive for Cloud Service Providers, TISAX, and FedRAMP Moderate.
- **Regular Testing**: Periodic network and application vulnerability and penetration testing are undertaken, with established procedures to document and address any discovered vulnerabilities.
- **Employee Training**: All employees are required to complete information security, data protection, and privacy training upon hire and annually thereafter.

Contractual Safeguards:

- **Data Processing Addendum (DPA)**: Elastic contractually commits to robust data protection and privacy measures under our Data Protection Addendum, which includes the SCCs and their Swiss and UK variants, as well as our Information Security Addendum. We regularly review and update our Data Processing Addendum to reflect applicable data privacy requirements and best practices.
- **Customer Instructions**: Customer Personal Data processing is strictly carried out only on customer instructions.
- **Confidentiality**: All personnel authorized to process Customer Personal Data are subject to stringent confidentiality agreements, policies, and procedures.
- **Control**: Customers retain the ability to retrieve, correct, or delete any personal data they upload to Elastic Cloud at any time.
- **Notification of Disclosure Requests**: Elastic contractually commits to notifying customers in the event of receiving a disclosure request for their data, unless legally prohibited from doing so.
- **Sub-processor Obligations**: We are fully transparent about our sub-processors, who are bound by the same stringent standards and organizational requirements. We're liable for the acts and omissions of our sub-processors to the same extent as if we performed the services ourselves.