



Elastic Transfer Impact Assessment

People's Republic of China

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Elastic product offerings, services, and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Elastic and its affiliates, suppliers, or licensors. The responsibilities and liabilities of Elastic to its customers are controlled by Elastic agreements, and this document is not part of, nor does it modify, any agreement between Elastic and its customers.

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. *We implement technical and organizational controls to prevent Elastic personnel located in the PRC from accessing the cloud admin console of cloud customers outside of the PRC.*

[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 direct access to 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 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.

PRC Transfer Impact Assessment

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

Applicable Government Access Legislation and Surveillance Scope

- **Complex Legal Framework:** The primary pillars are the **Cybersecurity Law (CSL)**, **Data Security Law (DSL)**, and **Personal Information Protection Law (PIPL)**. These are complemented by the **National Intelligence Law (NIL)** and various other regulations.
- **Data Security Law (DSL):** Enacted on June 10, 2021, and effective September 1, 2021. It applies to all data processing activities within China and has extraterritorial reach if activities harm China's national security or public interest. The DSL establishes a data categorization system: "National Core Data" (highest protection, impacting national security, economy, public interest) and "Important Data" (scope largely undefined, with catalogs expected from authorities). It mandates data localization for "core" and "important" data, particularly for Critical Information Infrastructure Operators (CIIOs).
- **Personal Information Protection Law (PIPL):** Enacted on August 20, 2021, and effective November 1, 2021. This comprehensive law regulates personal information processing by entities within China and extraterritorially for PRC residents' data. It requires consent for processing, including separate consent for cross-border transfers and sensitive personal information. PIPL broadly defines "Sensitive Personal Information" (SPI) to include biometric, religious, medical, financial, and location data. Cross-border transfers require a security assessment (for important data or large volumes), a standard contract, or certification. Recent amendments (March 2024) eased some requirements for non-important data and smaller volumes.
- **National Intelligence Law (NIL):** This law mandates that all organizations and citizens "support, assist, and cooperate with national intelligence efforts in accordance with law". This provision implicitly includes data access and has been interpreted by some experts as compelling Chinese telecommunications companies and potentially foreign subsidiaries to hand over data regardless of its origin.
- **Cybersecurity Law (CSL):** This law establishes a multi-level protection scheme for information systems and requires data localization for Critical Information Infrastructure Operators (CIIOs).

- **Government Access Procedures:** Requests for data from foreign law enforcement or judicial bodies generally require official approval from competent PRC authorities. Domestic law enforcement may assert jurisdiction over local branches of foreign organizations to access overseas data.

Assessment of Effectiveness of Transfer Tool & Legal Challenges

The volume and overlapping nature of the PRC's data laws (DSL, PIPL, CSL, NIL), coupled with vague definitions and extraterritorial reach, create a complex legal environment. A conflict arises from the DSL's explicit prohibition on providing data stored in the PRC to foreign judicial or law enforcement agencies without prior PRC government approval. This directly clashes with GDPR/UK GDPR obligations under SCCs to challenge unlawful requests and notify data subjects, creating a "data disclosure dilemma" that effectively "blinds" the data exporter to government access. If Elastic is legally prohibited from notifying a customer or challenging a request, it cannot fulfill its SCC obligations. This is a legal incompatibility at the core of data transfer principles, as highlighted by the EU General Court's Nuctech case. Furthermore, despite PIPL granting data subject rights, state agencies are largely exempt from PIPL, and judicial review of government data access is not robust. The NIL's requirement for entities and individuals to "support, assist, and cooperate with national intelligence efforts" suggests a potential for compelled, covert data access without warrants or transparency.

At Elastic, we are absolutely committed to ensuring the protection of our customers' data across all jurisdictions. We recognize that the PRC's legal framework raises important considerations for cross-border data transfers. Despite the complexity and extraterritorial reach of these laws, Elastic has determined that the use of the SCCs remains a valid and appropriate transfer mechanism. This determination is based on a detailed assessment and a risk-based approach consistent with EU guidance, including the principles established in the Schrems II ruling. We have implemented supplementary measures (below) that significantly reduce the risk of unauthorized access and ensure that transferred data continues to receive a level of protection that is essentially equivalent to that guaranteed under EEA law. While theoretical concerns around government access exist, there is no indication of any such access occurring in practice with respect to Elastic's services. Indeed, at this time, Elastic provides no cloud offering in the PRC, and offers only one hosting option in Hong Kong, available at cloud customers' sole discretion. We implement technical and organizational controls to prevent Elastic personnel located in the PRC from accessing the cloud admin console of cloud customers outside of the PRC.

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 explicit 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.
- **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.