# Elastic Transfer Impact Assessment

USA



*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 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) and Data Privacy Frameworks

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.

In addition, Elasticsearch, Inc. complies with the EU-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the "Data Privacy Framework") as set forth by the U.S. Department of Commerce. Elastic has certified to the Department of Commerce that it adheres to the Data Privacy Framework Principles with regard to the processing of personal data received from the European Union, United Kingdom, and Switzerland, as applicable, in reliance on the

Data Privacy Framework.

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.

# USA Transfer Impact Assessment

This section provides a detailed assessment of the legal and practical landscape for data transfers to The United States of America (USA), analyzing applicable government access legislation, the effectiveness of the SCCs, and Elastic's specific mitigating measures.

## Applicable Government Access Legislation and Surveillance Scope

The United States legal framework includes several statutes and executive orders that may enable government authorities to access personal data for national security, intelligence, and law enforcement purposes.

- **Foreign Intelligence Surveillance Act (FISA), Section 702:** This statute permits the U.S. government to direct "electronic communications service providers" (ECSPs) to cooperate in intelligence gathering activities. While the term ECSPs has been broadly interpreted by U.S. courts and the Department of Commerce to potentially include companies like Elastic, it is highly unlikely that U.S. intelligence agencies would target the ordinary commercial information Elastic processes for customers. Furthermore, Elastic is not eligible for "upstream" surveillance orders, which target internet backbone providers and were a principal concern in the Schrems II decision. To date, Elastic had not been subject to a U.S. government request under FISA 702.

- **Executive Order 12333 (EO 12333) & Presidential Policy Directive 28 (PPD 28):** Unlike FISA 702, EO 12333 does not grant the U.S. government authority to compel companies or individuals to disclose data. Surveillance activities under EO 12333 are subject to the restrictions outlined in PPD 28, which are designed to protect privacy and civil liberties. These restrictions include limiting bulk collection to specific national security purposes and minimizing the dissemination and retention of collected personal information. These restrictions are additional safeguards that reduce the likelihood of indiscriminate or unlawful search or seizure of personal data. To date, Elastic has not received any U.S. government requests under EO 12333.

- **The U.S. CLOUD ("Clarifying Lawful Overseas Use of Data") Act:** Enacted in March 2018, the CLOUD Act addresses conflicts regarding data stored outside the U.S. by requiring a court order to compel disclosure of such data under the U.S. Stored Communications Act (SCA). The SCA includes privacy safeguards that are preserved by the CLOUD Act. The Act also provides a mechanism for service providers to challenge requests that conflict with foreign privacy obligations. Elastic does not anticipate that the CLOUD Act will

 | 

have a practical impact on its handling of Customer Personal Data.

- **New Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities (October 7, 2022):** This Executive Order (NEO) introduces binding safeguards that limit access to data (including non-U.S. persons' data) by U.S. intelligence authorities to what is "necessary and proportionate" for national security. It mandates rigorous oversight, prioritizes targeted collection, and minimizes dissemination and retention. Crucially, the NEO establishes an independent and impartial redress mechanism, including a new Data Protection Review Court, to investigate and resolve complaints regarding data access by U.S. national security authorities. This development is considered to have "significantly increased" the level of protection for EU citizens' data in the U.S.

- **U.S. Federal Trade Commission (FTC):** The FTC plays a role in enforcing fair information practice principles (FIPPs) and has actively pursued legal actions against companies for privacy violations, imposing substantial fines.

- **U.S. Constitution (Fourth Amendment) and Electronic Communications Privacy Act (ECPA):** These legal instruments restrict the U.S. government's ability to compel service providers to disclose end-user information. They generally require subpoenas for basic user registration data and IP addresses, and court orders or search warrants for non-content records and communication content, respectively.

# Assessment of Effectiveness of Transfer Tool & Legal Challenges

The effectiveness of SCCs for data transfers to the U.S. has been a central point of contention following the Schrems II decision, which highlighted concerns about the breadth of U.S. surveillance laws. Historically, a primary challenge was the perceived broad scope of FISA 702 and EO 12333, which led the CJEU to invalidate the Privacy Shield. While Elastic's services are unlikely targets; the *potential* for broad interpretation of these laws presented a legal challenge to the effectiveness of SCCs, necessitating robust supplementary measures.

However, the landscape has fundamentally shifted with the adoption of the EU-US Data Privacy Framework (DPF) and the underlying New Executive Order (NEO). The NEO introduces binding safeguards that limit access to data to what is necessary and proportionate, mandates rigorous oversight, and establishes an independent redress mechanism, including a Data Protection Review Court. These developments directly address the core shortcomings identified in Schrems II, leading the EU Commission to grant an adequacy decision to the U.S. This means the U.S. is now formally considered to provide an "essentially equivalent" level of protection, as the European Commission re-confirmed in its latest periodic report on the functioning of the DPF (COM(2024)451 final, of October 8, 2024). This development significantly reduces the burden of demonstrating effective supplementary measures for transfers to the U.S., as Elastic's DPF certification is a strong indicator of compliance.

Given the nature and purpose of Elastic’s services, the Customer Personal Information that Elastic processes is highly unlikely to be requested under Section 702 FISA, EO 12333, or the CLOUD Act. We are not aware of any direct access to Customer Personal Data under EO 12333. We do not create or maintain backdoors or master

keys to our products or services, and we do not allow any government authority unfettered or direct access to our servers.

## 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.

- **Data Privacy Framework (DPF)**: Elastic is certified compliant with the Data Privacy Framework for personal data received from the European Union, United Kingdom, and Switzerland.
- **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.