Elastic Privacy Datasheet

Support Services

Service Summary: Elastic Support Services

Elastic Support Services provide a comprehensive system for customers to engage with Elastic for assistance with their Elastic products, including Elastic Cloud and self-managed deployments, as well as their related features and functions. Support Services are used to quickly address technical queries and resolve issues, leveraging both human expertise from a global team of Support engineers and AI-driven tools like the Support Assistant.

- **Product type:** Support Services
- **Deployment model(s):**
    - Hosted / managed

Data Processed in Elastic Support Services

Elastic Support Services process personal data as part of delivering the service. The specific types of personal data processed depend on the information provided by the customer during support interactions and the nature of the technical issue.

Categories of personal data necessary to access and use Support Services:

- Admin and user identifiers, credentials, permissions, session cookies, and activity logs. The processing of this data is essential for managing secure access and auditable use of the support system.
- Support contacts provided by the customer based on their subscription level.
- Business contact data collected when the customer contacts Elastic support, such as name, email address, and phone number.

Additional categories of personal data processed may include, but are not limited to, data contained within:

- Customer Personal Data contained within support cases and comments.
    - Examples: Information related to technical queries, issues, and communications exchanged with Elastic Support.
- Diagnostic files (run-time information and cluster metadata): The Support Diagnostic tool collects data about the health of nodes and other cluster metadata. This includes outputs from various Elasticsearch APIs and system calls. Depending on the customer's deployment(s) and infrastructure, such diagnostic data may contain information that could directly or indirectly identify customer end users. Elastic does not monitor or filter for such content, however:
    - The Support Diagnostic tool does **not** collect the actual source event or document data stored in your cluster.
    - Customers have the option to further sanitize diagnostic files by scrubbing out sensitive metadata such as IPs, hostnames, and index names prior to sharing with Elastic.
- Content from uploaded files for troubleshooting, such as heap-dumps, when explicitly authorized by the customer.
- Large Language Model (LLM) prompts and responses if the Support Assistant is used within the support context.

- Data from utilizing or arising from the use of generative and agentic AI features necessary or important to operate, optimize, improve, and monitor the performance of these technologies and/or meet regulatory and legal requirements.

Typical Purpose(s) of Processing Customer Data Shared with Support:

In general, Elastic Support Services are designed and intended for use cases such as:

- Facilitating communication and engagement between customers and Elastic Support to resolve issues and answer questions.
- Providing self-serve answers to technical queries using the GenAI-powered Support Assistant.
- Assisting with data ingestion, deployment scaling, and accessing meaningful insights to deliver business impact.
- Enabling case management including creating, reviewing, and updating support cases.
- Supporting collaborative problem-solving secure information exchange, including code snippets using Markdown or large file sizes.
- Diagnosing and troubleshooting technical problems by analyzing cluster performance, configuration, field mapping, and general cluster state using diagnostic files.
- Managing customer subscriptions and licenses.
- Providing expert advice and guidance for Elastic software through experienced Support engineers.
- Monitoring the efficacy and accuracy of our systems with User interactions.

Product Usage Data

Elastic Support Services, as part of the broader Elastic ecosystem, automatically collect certain information related to service usage. Such Product Usage Data is processed as described in the Elastic Product Privacy Statement.

Access to Customer Data

- **Access by Customers**: The Elastic Support Hub is fully integrated with Elastic Cloud. Existing subscription users access it with their Elastic Cloud account and can create and review support cases, get updates, download licenses, and check subscription information. All prior support data, including cases, comments, subscriptions, and licenses, remain accessible in the portal. All Elastic Cloud accounts can access the Support Hub, regardless of whether it has any running cloud deployments. Role-based access controls (RBAC) are integrated into Elastic deployments, allowing customer administrators to define roles that limit user access to specific information, enforcing least-privilege principles.

- **Access by Elastic**: Elastic Support typically handles "metadata" (indirect and non-identifying data) for troubleshooting, such as log files, configuration files, and product diagnostics, rather than actual Customer Content, Customer Personal Data, direct database, or end-user-identifying data.

    - In nearly all support or operational scenarios, Elastic's engineers do not access the content of customer data stored in data indices, nor do they have direct access to customer documents or file systems. Elastic will only access Customer Content in cloud deployments upon the customer's instruction, for instance, when providing support services at the customer's request. If an exceptional issue requires access to Customer Content (e.g., a heap dump), written authorization from the customer is mandatory. These processes are strictly controlled, fully auditable, and adhere to compliance standards like SOC 2 and ISO 27001.

    - The Support Diagnostic tool is used by Elastic Support to understand a customer's cluster health, but it does not collect actual source event or document data stored in the customer's cluster; it only collects run-time information and cluster metadata. This diagnostic output can be further sanitized by scrubbing sensitive metadata like IP addresses, hostnames, or index names prior to sharing with Elastic.

    - Elastic has implemented centralized logging, encompassing proxy logs, access logs, Elasticsearch logs, and Auditbeat logs to record all access to customer data and the systems on which it resides. Elastic's internal teams actively develop and implement detections for suspicious internal account activity and unauthorized access, including file integrity monitoring and account takeover indicators.

    - Elastic's principles dictate that it will only disclose or provide access to customer data when strictly compelled by law, and it includes established protocols for challenging such requests and notifying relevant parties where legally permissible.

Processing Locations

Support Services are provisioned through certain support sub-processors. These sub-processors are contractually bound to provide an equivalent level of data protection as Elastic. Elastic maintains full transparency regarding its sub-processors (see internal and external lists) and is liable for their actions and omissions to the same extent as if Elastic performed the services itself

Compliance with Privacy Regulations

Elastic captures, processes, stores, and protects Customer Personal Data in accordance with the applicable customer Data Processing Addendum, and the commitments outlined in this Privacy Data Sheet. Our Trust Center serves as a comprehensive resource for information on its privacy practices and compliance efforts.

- **Data Ownership:** Customer data remains the property of the customer. Elastic only processes this data for the purposes specified in the customer's agreement, and never sells customer data to third parties.

- **GDPR Compliance:** Elastic Support Services are designed for compliance with the General Data Protection Regulation and other global data protection and privacy laws. This includes prioritizing the security of personal data through effective technical and organizational measures, offering a GDPR-compliant Data Processing Addendum. Our dedicated privacy team at Elastic oversees GDPR compliance.
- **Data Privacy Framework (DPF):** Elasticsearch, Inc. is certified under 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 as set forth by the U.S. Department of Commerce.
- **Cross-Border Data Transfers:** Elastic also legalizes transfers of personal data originating from the EEA, Switzerland, or the UK by relying on current Standard Contractual Clauses, and its participation in the Data Privacy Framework for transfers to the US. Additionally, we implement robust supplementary measures to protect data during transfers, such as encryption in transit and at rest, protocols for challenging public authority requests, and providing customers with the option to select EU servers for hosting.

Retention and Deletion

Files uploaded to the Elastic Support Hub are automatically purged 30 days after upload to protect sensitive information. The ticketing system used by the Support Service removes all case attachments 15 days after case closure.

Security

The security of your data within Elastic Cloud relies on you keeping your deployments configured securely and maintaining the confidentiality of your Elastic Cloud login credentials (please see our Security FAQ for more information). In addition, Elastic supports a comprehensive defense-in-depth security model designed to protect customer data throughout its entire lifecycle: in transit, at rest, and in memory, as well as through robust key management procedures. Elastic also uses Elastic Security for its own internal InfoSec operations.

- **Encryption:** Customer data is encrypted at rest using AES-256 and in transit via TLS 1.2. Elastic implements strict encryption key management procedures.
- **Access Controls:** Elastic maintains technical, logical, and administrative controls to restrict data access solely to authorized users. These controls include measures such as multi-factor authentication, strong password strength standards, and the use of Virtual Private Networks (VPNs) for administrative access. Additionally, Role-based Access Controls (RBAC) are integrated into Elastic deployments and the Elastic Cloud management platform, allowing granular control over user permissions.
- **Logging and Monitoring:** Elastic has implemented centralized logging, encompassing proxy logs, access logs, Elasticsearch logs, and Auditbeat logs to record all access to customer data and the systems on which it resides. Elastic's Threat Detection and Response team utilizes automated workflows to detect and investigate suspicious internal account activity and unauthorized access.
- **System Updates and Patches:** Elastic systems are regularly updated and deployed based on the latest operating system kernels. Appropriate patches are applied promptly whenever a Common Vulnerability and Exposure (CVE) is identified in any software component.

- **Incident Detection and Response:** Elastic has implemented and continuously updates detection rules for suspicious activity and unauthorized access. These detections are part of automated workflows that alert the Threat Detection and Response team, triggering analyst investigations. Elastic uses Elastic Security internally which includes Endpoint Detection and Response capabilities and integrates threat intelligence feeds to support intrusion detection. It supports automated responses through integrations with third-party SOAR platforms, reducing the likelihood of a breach and speeding response times.
- **Secure Software Development Framework (SSDF):** Elastic maintains a secure software development framework based on NIST 800-218. This framework guides the process to securely design, develop, deploy, track, and maintain all Elastic software, ensuring a "secure by design" and "secure by default" approach.
- **Third-Party Vendor Review:** Elastic partners with major IaaS providers (AWS, GCP, Azure) and conducts rigorous reviews of their security and compliance standards, including SOC 2 audits and ISO 27001 certifications, as part of its third-party risk management program.
- **Penetration Testing:** Independent third parties conduct annual application and network penetration tests for Elastic Cloud. Elastic also hosts a public Bug Bounty Program for continuous researcher testing.
- **Employee Training:** All Elastic employees are required to complete comprehensive information security and data protection/privacy training upon hire and at least annually thereafter.