NETSCOUT Privacy Data Sheet

This Privacy Data Sheet provides an overview of how NETSCOUT processes personal data (or personally identifiable information).

Overview of NETSCOUT Product and Services Capabilities

NETSCOUT provides robust tools for the efficient and effective management of dynamic applications and comprehensive security of service-delivery network environments. Our proven application, network, and service intelligence offerings provide broad insight into the dynamic and real-time nature of critical data, video and voice services running across modern technology infrastructures. Our security solutions go beyond the traditional perimeter and endpoint protection to provide a comprehensive layered security architecture.

NETSCOUT's business assurance solutions, powered by our patented Adaptive Service Intelligence™ (ASI) technology, provide the visibility and insights you need to accelerate, transform, and innovate your networks and services for a flawless, agile, and cost-effective delivery.

Our DDoS and Advanced Threat solutions combined with ATLAS from Arbor, the security division of NETSCOUT, provide unparalleled visibility and threat mitigation both at the internet as well as the intranet level.

Please see https://www.netscout.com for a detailed description of our products and services.

The following paragraphs describe the personal data NETSCOUT processes in connection with the delivery of its solutions the location of that data, and how it is secured in accordance with privacy principles, laws and regulations. While this Privacy Data Sheet strives to provide an overview of all categories of personal data processed by NETSCOUT, there may be additional categories which are not described in this document.

1. Personal Data Processing

The table below lists the personal data used by NETSCOUT in connection with the delivery of its solutions and describes why NETSCOUT processes that data.

Personal Data processed by NETSCOUT	Purpose of Processing
Customer contact information for product and service administration	Creating an account, issuing of licenses, product notifications, training, support, product enablement, access to remote portals, and providing support in managed services.
Customer Submitted Files	Defect and/or mitigation analysis, support, and product enablement and improvement.
Customer Network Host Data	Defect and/or mitigation analysis and services for the purpose of product functions/operation. In the case of managed services offerings, such data will be used to manage the NETSCOUT infrastructure on customer networks.
Data contained in files provided for analysis	Defect and/or mitigation analysis, service and product enablement and improvement, and training.

Personal Data processed by NETSCOUT	Purpose of Processing
Customer Flow telemetry	NETSCOUT ARBOR SECURITY PRODUCTS Providing network behavioral modeling, threat detection, and anomaly detection function. Data collected is for product usage. The Arbor SP product collects flow telemetry records, which include source and destination address, number of bytes and packets and timestamps of IP traffic flows, as well as other information related to network infrastructure and traffic statistics. Network traffic statistics and DDoS attack data derived from flow telemetry is collected and processed in ATLAS cloud infrastructure. Shared statistics may be fully, partially, or non-anonymized based on the customer's discretion. ATLAS data is used to increase industry knowledge on DDoS and traffic trends through reports, industry sharing agreements, or other commercial mechanisms.
Customer packets	NETSCOUT ARBOR CLOUD Customer traffic is processed in NETSCOUT datacenters for the purpose of providing security mitigation services including DDoS mitigation services. Traffic is processed in real time with the service determining what to pass and what to drop. Raw traffic data is not stored long term.
Customer Device IP and Destination IP Addresses	NETSCOUT ARBOR SECURITY PRODUCTS Used for analysis while providing services and for managed services of the network.

2. Cross-Border Transfers

When a customer purchases a NETSCOUT nGenius or Arbor offering, all account information and licensing creation is processed in the United States. Arbor managed services are deployed from the United States and all systems used in providing those managed services are installed in the United States. NETSCOUT's VaaS (Visibility as a Service) is deployed in the United States for all systems based in the United States, in EMEA for all systems based in the EMEA region, or in APAC for systems based in Asia-Pacific region. In each case for VaaS, specific controls are in place which are designed to provide safety, security and privacy of personal data that is exchanged between these operations in accordance with NETSCOUT's security and privacy policies. NETSCOUT's product development, customer support, and managed service operations are located in various parts of the world, but specific controls have been implemented and are designed to provide safety, security and privacy of any personal data that is exchanged between these operations to enable efficient and world class services to our customers.

Our development, customer support, and managed service operations centers are located in the following countries: United States, Canada, countries in the European Union, Australia, India and China.

3. Access Control

Personal Data processed by NETSCOUT	Who has access	Purpose of the access
Customer contact information for product administration	Customers who own the data	Account administration
	NETSCOUT Employees – NETSCOUT Sales Administration, Licensing Operations, Product Operations, Engineering, Customer Support, and Managed Services.	Creating an account, validating license entitlements, general product operations, defect analysis, and customer support.
Customer Submitted Files	Customers	Customer support
	NETSCOUT Employees – Product Operations, Engineering, Customer Support, and Managed Services	Defect analysis and customer support.
Customer Network Host Data for product function/operation	Customers	Customer support
	NETSCOUT Employees – Sales Administration, Product Operations, Engineering, Customer Support, and Managed Services	Defect analysis, customer support, and managed services function.
Customer Username for Product function/operation	Customers	To manage users in their own organization.
	NETSCOUT Employees – Product Operations, Engineering, Customer support, and Managed Services	Defect analysis, customer support, and managed services function.
Data contained in files submitted for analysis	Customers	Defect analysis, customer support, and product improvement
	NETSCOUT Employees – Engineering, Customer Support, and Managed Services	Defect analysis, customer support, and product improvement

4. Data Retention

Customer Account Information Data
Customer account information data is currently retained indefinitely in NETSCOUT's U.S. data center. When a customer terminates its NETSCOUT subscription, it can specifically request that its data be purged from NETSCOUT's data center storage by opening a NETSCOUT TAC (Technical Assistance Center) case.

Samples and File Analysis Data
Trace files that are provided to NETSCOUT are retained for the purposes of fixing defects and making improvement to our solutions. These files are stored in encrypted servers in secure spaces within NETSCOUT development centers. These files are purged when a customer either ceases to be a customer of NETSCOUT or upon explicit request. NETSCOUT typically asks that customers provide trace files with only header information unless the full packet details are needed to resolve a support request.

Appliance Event Data
This data is used for the presentation of aggregate threat information in the ATLAS portal. A large portion of event data collected are behaviors, statistics and metadata extracted from customer deployments. Event data may be kept for mining, efficacy research, and threat intelligence purposes. This data is anonymized according to configuration chosen by the customer and stored indefinitely. When a customer terminates its NETSCOUT subscription, it can specifically request that this data be purged from NETSCOUT's data stores by opening a NETSCOUT ATAC (Arbor Technical Assistance Center) case.

5. Personal Data Security

The security of customer information is very important to NETSCOUT. NETSCOUT maintains a set of policies which establish a foundation for the privacy of all personal data used by NETSCOUT worldwide. These policies include but are not limited to (i) general principles regarding accessing, collecting, using, disclosing and retaining personal data, and (ii) physical, administrative, and technical safeguards designed to protect personal data from unauthorized access and use.

NETSCOUT takes appropriate security measures, consistent with international information protection practices, which are designed to protect customer protected information. These measures include, on our web sites and Internet-enabled technologies, administrative, technical, physical and procedural steps to protect personal data from misuse, unauthorized access or disclosure, loss, alteration, or destruction.

Personal Data processed	Type of Encryption
Customer contact information for product administration	Encrypted at rest
Customer Submitted Files	Encrypted at rest
Customer Network Host Data or product function/operation	Encrypted at rest
Customer Username for product function/operation	Encrypted at rest
Data contained in files submitted for analysis	Encrypted at rest
Appliance Event Data	Secured access but unencrypted at rest

6. Subprocessors

The list of subproccesors used by NETSCOUT in connection with the delivery of its solutions is available at www.my.netscout.com/mcp/security.