

GTT PRIVACY DATA SHEET

FOR Software-Defined Wide Area Network (SD-WAN) Service

SERVICE DESCRIPTION

This Privacy Data Sheet outlines how and why we process personal data in connection with GTT's SD-WAN Service (the "Service"). It provides details on where we store and transfer that personal data, how we maintain its security, and our compliance with relevant privacy laws and regulations. We will process personal data in accordance with this Privacy Data Sheet and with our [Privacy Policy](#).

The Service is a managed network overlay solution made available by GTT ("we," "us," and "our") to companies ("Client," "you," or "your") for their authorized users (each, a "user").

GTT's SD-WAN allows enterprise users to connect to any available transport and reliably connect to applications deployed on-cloud or off-cloud and offers enterprises enhanced global connectivity; optimized network availability and performance; and secure, end-to-end access to the applications that drive productivity and growth across the organization.

The solution utilizes GTT-provided and managed hardware and software located on client premises. The GTT core network hosts dedicated SD-WAN gateways along with a centralized management and configuration platform. GTT SD-WAN operates as a transport independent overlay across any last-mile access solution. The service creates a secure tunneled WAN to interconnect client locations, cloud applications and core GTT network services. GTT SD-WAN routes traffic across available access circuits based on business policies defined by the Client.

For a comprehensive understanding of the Service and its associated commitments, including Service Level Agreements (SLAs), please refer to the GTT Software-Defined Wide Area Network Schedule, available upon request.

TYPES OF (CLIENT) END USER DATA

- IP Address (source and destination)
- Hostname
- Login credentials (e.g., email address, username and security authentication data)
- Telephone number
- Technical support tickets may contain technical data shared by clients to assist in troubleshooting product-related issues
- Chat interaction data
- Device Information (e.g., MAC address, device name, unique identifiers)
- Network Information (e.g., Session, information, ISP name, public IP address, gateway IP address, transport protocol, destination port, destination fully qualified domain name, destination domain, application, application category, bandwidth, latency, packet loss and jitter)
- Other technical information (e.g., partition ID, Edge ID, enterprise ID, link ID, firmware information, virus statistics, URLs submitted for URL ratings (if supported), Antivirus, IPS, and Application Control Malware statistics, product serial number firmware version and information about updates)

PURPOSE OF PROCESSING (PROCESSOR)

- Service Provision
- Reporting, includes tracking
- Service Management
- Technical Monitoring
- Customer Support
- Troubleshooting

GTT

DATA DELETION & RETENTION

The table below lists the applicable retention periods for each category of personal data processed by GTT in connection to the Service.

Categories of Personal Data	Retention Period
End User Personal Data	If VMware (Broadcom) technology provider is used: - for the duration of the Agreement and at least twelve months If Fortinet technology provider is used, data retention and log storage shall apply for the duration of the Agreement and shall be subject to: (i) the Client's requirements, (ii) the retention period agreed between the Parties, and (iii) the Client's use of the log storage facility. If HPE Aruba (Silver Peak) technology provider is used, data retention and log storage shall apply for the duration of the Agreement and shall be subject to: (iv) the Client's requirements, (v) the retention period agreed between the Parties, and (vi) the Client's use of the log storage facility. If Palo Alto Networks technology provider is used, data retention and log storage shall apply for the duration of the Agreement and shall be subject to: (vii) the Client's requirements, (viii) the retention period agreed between the Parties, and (ix) the Client's use of the log storage facility. -

GTT

DATA LOCATION & STORAGE

Storage Location (Subprocessors)	Access Location
VMware (Broadcom) hosted database in the US	GTT Personnel: Authorized personnel located in Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location. Sub-processor: Authorized sub-processor personnel with authenticated access into the appropriate management platform depending on their country location.
HPE Aruba– the location is agreed with the client out of the following: UK (Slough), UK (London), US (Dallas), US (New York), US (Los Angeles), US (Chicago), US (Atlanta), Canada, the Netherlands, Sweden, Germany (Frankfurt), Germany (Berlin), Switzerland (Zurich), Switzerland (Geneva), France, Italy, Spain, Hong Kong, Japan, Singapore, Australia, South Africa, Brazil. For clients using offerings that include Aruba Orchestrator as a service, please refer to the Aruba Privacy Data Sheet.	GTT Personnel: Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location.
Fortinet – the location is agreed with the client out of the following: UK (Slough), UK (London), US (Dallas), US (New York), US (Los Angeles), US (Chicago), US (Atlanta), Canada, the Netherlands, Sweden, Germany (Frankfurt), Germany (Berlin), Switzerland (Zurich), Switzerland (Geneva), France, Italy, Spain, Hong Kong, Japan, Singapore, Australia, South Africa, Brazil.	GTT Personnel: Authorized personnel located in Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location.
Palo Alto - – the location is agreed with the client out of the following: UK (Slough), UK (London), US (Dallas), US (New York), US (Los Angeles), US (Chicago), US (Atlanta), Canada, the Netherlands, Sweden, Germany (Frankfurt), Germany (Berlin), Switzerland (Zurich), Switzerland (Geneva), France, Italy, Spain, Hong Kong, Japan, Singapore, Australia, South Africa, Brazil. For clients using offerings that include Palo Alto Orchestrator, please refer to the Palo Alto Data Sheet. -Palo Alto SD-WAN	GTT Personnel: Authorized personnel located in Bulgaria, India, and USA or other locations with authenticated access into the appropriate management platform. Client: Authorized Client employees, contractors, representatives and end-users depending on their country location.



PERSONAL DATA TRANSFER

To ensure compliant data transfers across jurisdictions, GTT has established an Intra Group Data Transfer Agreement (IGDTA) between GTT's entities. This agreement utilizes the EU Standard Contractual Clauses and other applicable data transfer mechanisms as needed to maintain lawful and secure data processing practices.

ACCESS TO PERSONAL DATA

Users, Client, and GTT can access personal data in connection to the Service as described in the table below.

Parties with Access	Justification	Access Control
GTT personnel	Troubleshoot, support Service and report.	Corporate Credentials and MFA
Client	Through appropriate management platform with access limited to only that Client's End User Personal Data	Client Credentials and MFA (may be available depending on the technology provided)
Sub-processors	Troubleshoot and support Service	Corporate Credentials and MFA



THIRD-PARTY SERVICE PROVIDERS (SUB-PROCESSORS)

Below is a list of third-party service providers that GTT may use to deliver the service, along with links to their respective privacy policies.

Third-Party Suppliers	Country	Supplier's Privacy Statement
VMware (Broadcom)	Global	Broadcom Privacy and Data Protection
HPE Aruba (Silver Peak)	Global	HPE Privacy Statement HPE Aruba Orchestrator
Fortinet	Global	Fortinet Privacy Policy Fortinet Data Privacy Practices
Veeam	Switzerland	Veeam Privacy Notice Veeam Data Processing Addendum
Palo Alto	Global	Palo Alto SD-WAN Palo Alto Privacy Statement
Arista	Global	Arista Privacy Policy Arista Data Privacy Addendum