

GTT PRIVACY DATA SHEET

FOR Managed Detection and Response Service

SERVICE DESCRIPTION

This Privacy Data Sheet outlines how and why we process personal data in connection with GTT's Managed Detection and Response 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 an outsourced cybersecurity service made available by GTT designed to protect data and assets of its clients and their authorized users from threats that evade common organizational security controls.

For a comprehensive understanding of the Service and its associated commitments, including Service Level Agreements (SLAs), please refer to the GTT Managed Detection and Response Schedule, available upon request.

TYPES OF (CLIENT) DATA

Categories of Personal Data	Types of Personal Data
Mandatory categories of personal data processed as part of the service	A) User Information: • First and Last Name • Address • Email Address • User ID • Domain • Domain Name • User Internet Protocol (IP) Address or Subnet B) Integration information:

	• Usernames • API Keys • API Locations/Hosts • License Details C) User search information: • IP Address • Email address • URL • Domain name • File path/file name • Email/Email subject • Username or ID • Other personal information processed in relation to a user search D) Network flow Metadata • IP address (source) • IP address (destination) E) Network Access Control (NAC) Session Data • Device type • Active Directory (AD) session data • Device Operation System (OS) information • Mobile Device Management (MDM) status • Adaptive Network Control (ANC) policy F) Events, Alerts and Observations related information: • Username, User ID, email address, asset groups • URLs accessed by an end-user • IP Address (user, source, destination) and MAC Address • File name • Host name • Event type • Organizational unique identifier • Fully qualified Domain Name • DHCP information • Browser user agent information • Other event details contained by reporting product G) Asset data: • IP address • Host/device name • MAC address • Device geolocation • Device activity timestamp
--	--

	• Device configuration settings • MDM data H) Usage data: • Names • User ID • Email address • User address (country and city) • Session Data • MDR Product usage data related to web-browser activity • Personal data inserted by a user in a free text field or survey response as part of providing feedback.
Optional categories of personal data processed depending on Client's usage and agreed supplementary services	• IP Address (end-points) • Host ID • User ID and/or user name • Media Access Control (MAC) Address • User Passwords • Destination Host Name for Applicable Firewall • Domain Name System (DNS) Information • Additional network activity which is contained within the network logs (e.g., URLs visited by users) • Initial Data Packet (IDP) which main contain an IP header, TLS header, Server Name Identifier (SNI), Cipher suites including certificate, organization, issuer, issued and expiration • User data • IP address (user) • Device host name • Passive DNS logs • Tags and comments

PURPOSE OF PROCESSING (PROCESSOR)

- Service Provision
- Reporting
- Service Management
- Technical Monitoring



- Customer Support
- Troubleshooting

DATA DETENTION & 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
Client Personal Data	12 months unless extended by Client contract

DATA LOCATION & STORAGE

Storage Location	Access Location
United Kingdom (UK) data centre	GTT personnel located in UK
United States data centre	Back up of the UK data center.

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

Authorized 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 located in UK	Troubleshoot and support Service	Corporate Credentials and MFA
Client	Through appropriate management platform with access limited to only that Client's End User Personal Data	Client Credentials, MFA (available)



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
LogRhythm	Global	https://logrhythm.com/privacy-statement/