Data Processing Annex for BT Managed Cloud Security - Cisco Service

A Note On 'You'

'You' and 'your' mean the Customer.

Data Processing Annex

1 Subject Matter Of The Processing Of Personal Data

This Data Processing Annex sets out the details regarding how Customer Personal Data is Processed when providing the BT Managed Cloud Security - Cisco Service.

2 Duration Of The Processing Of Personal Data

BT or its Sub-Processor will Process the Customer Personal Data for the BT Managed Cloud Security - Cisco Service as set out in this Annex for as long as BT provides the BT Managed Cloud Security - Cisco Service and for as long as BT may be required to Process the Customer Personal Data in accordance with Applicable Law.

3 The Nature And Purpose Of The Processing Of Personal Data

3.1 The Service allows you to set rules by which URLs are blocked and web content is filtered on your IT systems. The software itself is provided by a third party and hosted on that third party's public cloud infrastructure, with no access to underlying information possible for BT.

3.2 If you request a 'management overlay', BT will have access through Cisco's online portal to the Personal Data set out in Table 1 of this Data Processing Annex, in order to provide reports to you, for day to day management and creating rules for the Service. BT will only have access to data contained within Cisco's online portal (including when a customer managed Amazon S3 Bucket Service is configured for log storage).

3.3 For the provision and management of the Service by Cisco, any Processing of Personal Data will be subject to the Cisco's Master Data Protection Agreement and the types of Customer Personal Data Processed by Cisco will be as set out in the Cisco Umbrella Privacy Data Sheet: file:///C:/Users/611061810/OneDrive%20-%20BT%20Plc/Product/Cisco%20Umbrella/Global/Data%20Protection/umbrella-privacy-data-sheet.pdf as may be amended or supplemented from time to time by Cisco.

3.4 "**Amazon S3 Bucket Service**" means an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects.

3.5 "**Cisco**" means Cisco International Limited registered in England and Wales (Company Number 06640658), having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom and Cisco Systems, Inc., with its principal place of business at 170 West Tasman Drive, San Jose, CA 95134 (together "Cisco")

3.6 "**Cisco's Master Data Protection Agreement**" means Cisco's Master Data Protection Agreement at https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf as may be amended or supplemented from time to time by Cisco.

4 Types Of Personal Data and Categories of Data Subjects

4.1 The types of Customer Personal Data Processed by BT or its Sub-Processors or you will be as set out in Table 1 to this Data Processing Annex.

4.2 The Customer Personal Data will concern the following categories of Data Subjects:

4.2.1 your employees;

4.2.2 your customers or third parties; and

4.2.3 any Data Subject (as controlled by you).

Table 1

Personal Data Category	Types of Personal Data Processed
Account/Contact Information	• Dashboard/console user email address and name • Company account information (Company name, street, city, state/region, country, phone number, Unique numerical account ID) • Billing contact name
DNS Layer Security1 Usage and Event Data	• Personal data contained in DNS query data (IP address/origin IP, destination domain name) • Personal data contained in DNS logs (IP address/origin ID, destination domain name, DNS record type, DNS response) • Device ID • Cloud apps associated with user or device
	If using DNS block page: HTTP/HTTPS header info and URL, excluding HTTP/HTTPS body content
	If using optional selective proxy feature: • Personal data included in web traffic (HTTP/HTTPS) that is intercepted and proxied by selective proxy (i.e., traffic associated with certain uncategorized or risky domains), including personal data in headers, URLs, and body content (e.g., files) • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs (however only query parameters for HTTP traffic and not for HTTPS traffic are logged) • Cloud apps associated with user or device
Secure Web Gateway1 Usage and Event Data	• Personal data included in web traffic (HTTP/HTTPS), including headers, URLs, and body content (e.g., files) • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs (however only query

	parameters for HTTP traffic and not for HTTPS traffic are logged) • Cloud apps associated with user or device
Cloud-Delivered Firewall Usage and Event Data	• All personal data included in ports and protocol meta information including packet content, source IP and port, destination IP and port, application (e.g., Webex), date, and timestamp
Cloud Malware Usage and Event Data	• User ID and/or e-mail address • User first and last name • IP Addresses for end users • Any other personal data that may be inspected for malware because it is stored on the applicable cloud environment
Data Loss Prevention Usage and Event Data	• For SaaS API-based DLP and Real-Time DLP • File name (if includes personal data) • Personal data in files, messages or other content inspected by DLP • Snippet of policy violation and surrounding text if policy violation detected • For SaaS API-based DLP: • the email address and display name of users in customers' cloud (SaaS) environments that will be monitored with such service • email address and display name of collaborators of a changed file • File id of file detected to contain data violations • For Real Time DLP: leverages Umbrella identity data from Secure Web Gateway (see Configuration Information)
Remote Browser Isolation	• Session ID (numeric session identifier) • Browser configuration (e.g., browser type, version, local settings, window dimensions, operating system, etc.) • Any other personal data contained in user requests or user input in the isolation platform • Any other personal data present on pages that are isolated by the platform • User configuration (random numeric identifier and other browser information

	collected by persistent cookies to store browser configuration information)
Configuration Information	• Audit logs (administrator name) • Policy settings (administrator name, IP address) • Object labels (object labels such as network, roaming computer and mobile device names) • Chromebook client ID (email ID) • Unique account ID
	For SaaS API-based DLP: • OAuth Keys (token ID and password) • usernameof admin that authorized access • email address and display name of all users in customer's SaaS environments that will be monitored with such service.
	For Cloud Malware: • OAuth Key (token ID and password) • username of admin that authorized access
	• If using Active Directory or another cloud Identity Provider (IdP) integration add-on: User identity (first name, last name, username, display name, email, GroupName) • If using Active Directory add-on: Device id, Device name, UserID, GroupID
Dashboard Activity Information	• Dashboard users' first and last name, email address, IP address, userID, country, region, city, role • Dashboard users' device information: device name, device type • Dashboard activity usage metrics • OrgID
Support Information	• First and last name • Email address • Phone number of the employee(s) appointed to open the service request • Customer account information: (Company name, street, city, state/region, country, Unique account ID)

Business and Product Usage Analytics	• Product usage, contact and user information, which may include the following types of personal data of the dashboard user: • First and last name, • Job title • Permission Role • Company name • Physical address (street, city, state/region, country) • Email address and corresponding unique numerical account ID • Username and/or ID • IP address • Phone number • Device type and device name • Timestamp for login