Colt IP Guardian – DDoS Protection, Data Protection Sheet

This Data Protection Sheet describes the details of the personal data processing activities derived from Colt IP Guardian service (the "Service") execution.

What is this Service about?

Colt IP Guardian is a **Managed Cybersecurity Service**, an add-on service which provides protection for an underlying Colt IP Access from Distributed Denial of Service cybersecurity threats.

Colt IP Guardian alerts on malicious traffic destined for a customer on the Colt network and then applies technical mitigations and countermeasures within Colt network to filter out the malicious traffic. An automated mitigation option and a manual mitigation option are offered, both which can be controlled by the customer in the IP Guardian Customer Portal, which provides a control panel that gives real-time and historical reports on DDoS events and also permits Customers to tailor the way the mitigation is applied to optimise the service against dynamic threats.

The Service is provided directly by Colt to its customers ("Customers") for use by the customer and the customer's portal administrators (each an "End User"). Colt may process the customer and the customer's end user personal data in the process of the Service.

Data Protection Colt's Role

For this Service, Colt as a Telecommunication Services Provider considers itself as an independent Data Controller as defined by Article 4 (7) of the GDPR, as it 'determines the purposes and means of the processing of personal data'.

As a Business to Business (B2B) Telecommunication service provider, Colt processes 'Business Contact Personal Data of Customer's personnel' for the execution of the contract with the Customer from pre-contractual to post-termination stages, to comply with certain regional legal compliance obligations (tax, etc.), including obligations requested as a Telecom Service Provider (such as legal interception or disclosure).

Legal basis and purposes of the Personal Data processing

Contract Execution	Execution of the contract between Colt and Customer, including pre-contractual commercial relationship (prospect campaigns, marketing), contractual relationship (contracts, Master Service Agreements, General Terms and Conditions, negotiation, signature, order management, invoicing and billing, CRM, product/service provision (installation, delivery, activation, maintenance, troubleshooting, customers portals

	(e.g. Colt On Line), incident management, quality management) and post-contractual relationship (credits and collection, CRM, marketing)
Legal obligation	Legal obligations, such as regulatory, legal interception, accountability, commercial and tax obligations
Legitimate Interest	Ensure the security of the network

Categories of Personal Data processed and type of Personal Data

Business contact data (Job title, name, last name, ID number, company phone number, company mobile number, company email, signature).
ID number, User_Name assigned to an entity/customer to allow a customer administrator access to the IP Guardian Customer Portal on the multi-tenant platform.
Corporate Email to send alerts generated by the service to the customer when an attack begins and Colt starts to protect their service.

Other Information which does not identify individuals

IP Address that was the target of malicious traffic coming from the internet, to report both current and historical DDoS alerts and associated malicious traffic analysis. By default, the Product doesn't process or store unique IP addresses that are identified as associated with a specific data subject or any actual traffic data payload unique to an individual IP address.
Logs stored by the service are purely information about customer's traffic pattern to identify any suspicious attack, no personal data identifiable. These logs will be stored for reporting and analysis if an alert has occurred.

Categories of data subjects

Colt and Customer's employees using or managing the Product/Service or the contractual relationship who are natural persons.

Duration of the Processing

In general terms, personal data is retained no longer than the minimum time needed to comply with tax and legal obligations and enforce our Service agreements, according to legal, tax and statutory requirements specified under the applicable laws and regulations. In particular, IP Addresses and Logs are stored for 90 days so that the customer and Colt's Cybersecurity Operation Centre (CSOC) teams can analyze attacks and the effectiveness of the service. This is only kept to allow the service to function. No actual customer data is stored as only metadata about the alert is generated and stored by the service.

Locations where personal data is processed and stored

Organizations with authorized access to customer data	Storage location	Access location	Legal Measures (BCRs, DPA, SCC, Privacy Statements, etc)
Colt Group	Service Platform located in UK	Colt CSOC and Technical Assistance Center support teams, located in India and Germany	European Binding Corporate Rules (BCRs) as Controller and Processor
Customer		Access remotely to the IP Guardian management platform	

Legal measures and statements

Colt complies with the transparency principle mainly through its publicly available Data Privacy Statement.
Colt processes as an independent controller of Business Contact Personal Data of Customer's personnel in compliance with data protection rules and within the terms described in Colt Compliance Statement
Colt has embedded the Privacy by Design and by Default principle, incorporating it into the data processing activities of Colt
Colt has been awarded Binding Corporate Rules ('BCRs') certification for both controller and processor. Colt's BCR Controller and Processor decisions are published at the European Data Protection Board ('EDPB') website and at the Spanish Data Protection Authority ('AEPD') website. BCRs are a certification granted by the EDPB, the collective body of all European Union ('EU') Data Protection Authorities. Through the BCRs, the EDPB certify that the privacy program implemented by a company is compliant with the GDPR and the same level of data protection compliance valid in Europe is applied all over the entities of the same group. In addition, the BCRs are a tool for safely transfer personal data outside the EU within a group of companies.

Certifications

SL No	**Certification**	**Name**	**Link**
1	ISO/IEC 27001:2013	Information Security Management	https://www.colt.net/why-colt/certifications
2	ISO 9001:2015	International Quality Management System	
3	ISO/IEC 20000-1:2018	Service Management	
4	ISO/IEC 14001:2015	Environmental Management	
5	ISO/IEC 22301:2012	Business Continuity Management	
6	Cyber Essentials	Cyber Essentials	
7	ISO 27701	An extension of ISO/IEC 27001 and ISO/IEC 27002 for Privacy	