Colt SD WAN – Data Protection Sheet

This Data Protection Sheet describes the details of the personal data processing activities derived from Colt Software-Defined Wide Area Network (SD WAN) service (the "Service") execution.

What is this Service about?

SD WAN is a specific application of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technology applied to Wide Area Network (WAN) connections, which are used to connect enterprise sites.

SD WAN enables public Internet to be used as an access mechanism to a Customer site, stand-alone or complementing the existing Multiprotocol Labelling Switching (MPLS)-based IP Virtual Private Network (VPN) access.

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 as detailed below in a data protection controller role.

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, for any Personal Data processed by Customer and Colt in connection with this Product, such as: (i) contact information of each Parties, (ii) any Personal Data of the signatories of the contracts executed by the parties or Personal Data provided by the Customer and (iii) Colt to execute the Contract and/or provide the Product/Service, i.e. 'Business Contact Personal Data", each party is an **independent Data Controller** and will comply with their respective obligations under the Data Protection Laws.

Legal basis and purposes of the Personal Data processing

Contract Execution	Execution of the contract between Colt and Customer for administration purposes, 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) for administration purposes.

Categories of data subjects

Colt and Customer's employees Business Contact Personal Data for administration purposes.

Duration of the Processing

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.

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	Several countries globally.	Several countries globally	European Binding Corporate Rules (BCRs) as Controller and Processor

Colt used Sub-processors (third party suppliers)

Colt does not use third-party suppliers, different than the ones for setting up and/or delivering the services and Other Local Telco Operator providers, when needed, to provide the Services, as the underlay for SD WAN services is Internet and Multiprotocol Label Switching (MPLS) connectivity.

For collateral services provided by Versa and Vmware, such subcontractors do not process any personal data of Colt´s Customers.

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.
Colt has achieved ISO 27701:2019, an extension of ISO/IEC 27001 and ISO/IEC 27002 for Privacy and Personal Data. This **Global standard** provides the framework for organizations looking to put in place a system to support compliance with the EU's GDPR, California's CCPA, and other data privacy requirements. ISO 27701, also referenced as PIMS (Privacy Information Management System), outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy.

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	

Updated : April 2024