

Colt WAVE – High Bandwidth Optical Connectivity

Data Protection Sheet

This Data Protection Sheet describes the details of the personal data processing activities derived from Colt Wave (the “Service”).

Colt Wave Services are part of the **Optical Services** range, which enable high bandwidth network connections to be deployed quickly and easily over Colt’s high capacity, scalable optical infrastructure.

Colt Wave Services provide high-capacity data transport services between two locations. They are available on a Metro, National or International basis. Colt owns and operates fully managed and integrated metropolitan and long-distance networks, based on fibre-optic infrastructure, which facilitate secure, high-bandwidth Dense Wavelength Division Multiplexing (DWDM) connections across the network. Intercontinental services, global locations in North America and international services in the Asia Pacific region are served using leased wavelength capacity in combination with Colt’s own optical infrastructure.

The Service is provided directly by Colt as a telecommunications or communication service provider to its customers (“Customers”). A telecommunications or communication service provider is company that transports information electronically through telephony and data communication services in the networking industry. Colt is also an Internet Service Provider (ISP).

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
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 contact 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. Colt servers are located in the UK & EU (Netherlands/Frankfurt).	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 Local Telco Operator providers, when needed, according to Telco regulations.

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.

Cot Technology Spain has been awarded by the highest level of the [Spanish Nacional Security Scheme Certification \(ENS\)](#) to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of the data, information and services used by electronic means that they manage in the exercise of their competences Royal Decree 311/2022

Certifications

SL No	Certification	Name	Link
1	ISO/IEC 27001:2022	Information Security Management	https://www.colt.net/why-colt/certifications
2	ISO 9001:2018	International Quality Management System	
3	ISO/IEC 20000-1:2018	IT Service Management	
4	ISO/IEC 14001:2015	Environmental Management	
5	ISO/IEC 22301:2019	Business Continuity Management	
6	Cyber Essentials	Cyber Essentials	
7	ISO 27701:2019	An extension of ISO/IEC 27001 and ISO/IEC 27002 for Privacy	

Updated : October 2024