Privacy by Design and Default measures implemented by Colt

TO WHOM IT MAY CONCERN

Colt has embedded the Privacy by Design and by Default principle incorporating it into the data processing activities (systems, services, policies & products) of Colt, taking into account the privacy throughout the life of Colt data processing cycle, allowing Colt to anticipate and protect privacy against the negative and invasive effects of new products and technologies in an initial point, starting from the minimization of data, both in the amount handled, treatment, period of storage and accessibility.

In addition, Colt has implemented tools and checks to analyse and ensure that any personal data processing follows a Privacy by Design and Default policy, as well as tools to ensure the lowest possible risk, allowing the protection of fundamental rights and freedoms of the data subjects. **Colt has implemented the following Privacy by Design and Default measures:**

- **Data Minimization:** data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- **Controllability:** an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding con-sent and objection should be supported by technological means.
- **Transparency:** both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
- **User Friendly Systems:** privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- **Data Confidentiality:** it is necessary to design and secure IT systems in a way that only authorized entities have access to personal data.
- **Data Quality:** data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes. At Colt, the data collection forms are drafted appropriately to ensure that excessive personal data is not collected. Regular checks are implemented to ensure personal data accuracy are carried out.

- **Use Limitation**: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data ware-houses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

- **Ropa and Data Mapping: Use Limitation:** Personal data is appropriately mapped, classified, labelled, stored and accessible as per the Data Mapping and the Record of Processing tool implemented by Colt.

- **Retention and Destruction Policy:** There is a Retention and destruction Policy that determines the deletion periods and how data shall be destroyed depending on the media. Deletion certificates must be fulfilled after every erasure for audit purposes according to such policy and an audit is implemented for such purposes.

- **Use, Retention, and Disclosure Limitation** –Colt process personal data in accordance with this principle, by which the processing of personal data should be limited to the relevant purposes identified to the individual, for which he/she has consented, except where otherwise required by law. Colts conduct a Light Impact Assessment to evaluate such purposes as well Data Privacy impact assessment through PIAs that contain comprehensive information on personal data, use, collection and retention as well as legal controls implemented and security measures.

- **Information Principle:** Colt has implemented a Data Privacy statement to inform our customers on how Colt processes personal data, why, customer rights and all other information required under the data privacy legislation.

- **Mandatory Training:** All employees have been trained on aspects of data security. We conduct mandatory training assessments for employees.

- **Vendor Assessment:** When Colt onboard a new vendor conducts a vendor privacy assessments including security and data privacy controls and KPIs.

- **Privacy as a default setting:** Colt considers privacy as the default setting, ensuring personal data is automatically protected in all IT systems or business practices, with no added action required by any individual. We approach to this requirement as follow:

  •Purpose Specification –Specified purposes should be clear, limited and relevant to the circumstance and shall be communicated to the individual (data subject).

  •Collection Limitation – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

  •Data Minimization – the collection of personally identifiable information should be kept to a strict minimum.

- **Ensure end-to-end security**: Colt considers data lifecycle security therefore all data should be securely retained as needed and destroyed when no longer needed.
    - Regarding security – Colt entities assume responsibility for the security of personal information) throughout its entire lifecycle.
    - Colt applies security standards to the confidentiality, integrity and availability of personal data throughout its lifecycle including, methods of secure destruction, appropriate encryption, and strong access control and logging methods.
    - Colt has implemented the below TOM measures, certifications and controls:

        - Measures of pseudonymization and encryption of Personal Data.
        - Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services.
        - Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
        - Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing.
        - Measures for user identification and authorization.
        - Measures for the protection of Personal Data during transmission.
        - Measures for the protection of Personal Data during storage.
        - Measures for ensuring physical security of locations at which Personal Data are Processed.
        - Environmental controls in facilities storing Personal Data.
        - Processes for ensuring that Personal Data is only hosted in facilities with the highest guarantees and certifications (ISO 27001:2013, SOC 2 Type II, etc.).
        - Adherence to widely recognized standards including but not limited to ISO 27000, ISO 2230, and SOC
        - Maintenance of relevant certifications such as ISO 27001 for Information Security management system (ISMS), ISO 22301 for Business Continuity Management System (BCMS), SOC 2 Certification, and/or PCI DSS for card holder environments.
        - Implementation and maintenance of an information security management program based on generally accepted frameworks such as the ISO 27000, NIST Cybersecurity, and CIS Controls, including but not limited to, mobile device policies, incident response management policies, teleworking policies, acceptable use policies, asset management policies, and change management policies.

- **Privacy and Security certifications**

- Colt has been awarded **BCRs of controller and processor by the European Data Protection Board (EDPB)** August 02, 2021. The approval was published in the official Gazette of the EDPB on August 05, 2021 and ratified by the Spanish Data Protection Authority, as Colt´s BCR leading Authority. Colt´s BCRs were negotiated and discussed with the Spanish Data Protection Authority, Hesse Data Protection Authority and French Data Protection and approved by the European Data Protection Board which includes all the EU Data Protection Authorities. The BCRs are the only available instrument to get company´s data privacy practices and program approved by the EU Data Protection Authorities. Colt´s BCRs allows Colt to transfer EU personal data within the Group, even outside the EEA, recognizing a Global Privacy

programme that meets highest possible industry standards. For approving our BCRS, the EDPB audited, validated and approved Colt privacy compliance framework applicable in all Colt´s entities and implemented by Colt across the whole group. The approved privacy programme is legally binding on every company of the group.

- Furthermore, in accordance with EDPB request, Colt has consulted four Data Protection Authority (Hesse, CNIL, AEPD, Garante) regarding the supplementary measures and roadmap included in the Privacy by Design Policy and the conditions requested to be effective. Due to such consultation, Colt has agreed further commitments which have being included in Colt´s BCRs documents approved by the EDPB as detailed above and implemented throughout Colt´s group.
- Colt adheres to the Telecommunications Code of Conduct approved by the Austrian Data Protection Authority (DSB).
- Colt is certified to ISO/IEC 27001 – Information Security Management System (ISMS).
- Colt is implementing the ISO 27701 an extension of ISO/IEC 27001 and ISO/IEC 27002 for Privacy.
- Colt operates a number of **security policies** including but not limited to:
    - Colt Information Security Policy
    - Colt Information Classification and Handling Policy
    - Colt Background Screening Policy
    - Colt Physical Security Policy
    - Colt Internal Acceptable Use Policy
    - Colt Password Standard
    - Access Control Policy
    - Network Security Policy
    - Physical security Policy
    - Business Continuity Policy
    - Colt Malicious Software Policy
- The following are the list of certifications Colt currently holds:

SL No	Certification	Name	Link
1	ISO/IEC 27001:2013	Information Security Management	https://www.colt.net/why-colt/certification
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	

Alessandro Galtieri

Group Data Protection Officer & India Grievance Officer

COLT TECHNOLOGY SERVICES

June 2023