SPANISH DATA PROTECTION AUTHORITY

DECISION APPROVING BINDING CORPORATE RULES FOR CONTROLLERS OF COLT GROUP

1. Having regard to Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), the Spanish Data Protection Authority shall approve Binding Corporate Rules (BCRs) provided that they meet the requirements set out under this Article.

   Whereas:

2. In accordance with the cooperation procedure as set out in the Working Document WP263.rev.01, the Controller BCR application of COLT Group were reviewed by the Spanish Data Protection Authority, as the competent Authority for the BCRs (BCR Lead) and by two SAs acting as co-reviewers. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.

3. The review concluded that the Controller BCR of COLT Group comply with the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256.rev.01 and in particular that the aforementioned BCR:

   i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCR all of which is set forth in the Group´s **Intra-Group Agreement** passed by all the companies affiliated to the BCRs.

   ii) Expressly confer enforceable third party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCR. **(Intra Group Agreement and Section 9.1 of the Controller BCR**).

   iii) Fulfil the requirements laid down in Article 47(2):

   a) The structure and contact details of the group of undertakings and each of its members. **(Appendix 3 of the Controller BCR)**.

   b) The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the categories of data subjects affected,

and the identification of the third country or countries. **(Section 1.2 and 2 of the Controller BCR)**.

c) The legally binding nature of the BCRs, both internally and externally. **(Section 1 of the Controller BCR, Intra-Group Agreement)**.

d) The application of the general data protection principles, in particular, purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data. **(Sections 3, of the Controller BCR).**

,

e) The measures aimed at guaranteeing data security and the requirements regarding subsequent transfers to bodies not bound by the binding corporate rules. **(Section 4, 5, 6 and 7 of the Controller BCR)**.

f) The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules. **(Section 9 of the Controller BCR)**.

g) The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the Group not established in the Union, as well as the exemption of the controller or the processor from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage. **(Section 9.2 of the Controller BCR)**.

h) The way in which information about binding corporate rules is provided to data subjects. **(Section 9.3 of the Controller BCR)**.

i) The tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, as well as monitoring training, complaint-handling and the claim procedures **(Section 7.2.3 and 8.1 of the Controller BCR).**

j) The claim procedure. **(Section 8.1 of the Controller BCR).**

k) The mechanisms established within the group of undertakings to verify compliance with the binding corporate rules. Such mechanisms shall include data protection audits and systems for ensuring corrective actions to protect the rights of data subjects. The results of such verification must be reported to the Data Protection Officer, as well as to the Group Management, and shall be available upon request from the competent data protection authority**. (Section 8.4 of the Controller BCR).**

l) The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority**. (Section 13 of the Controller BCR)**.

m) The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of verifications. **(Sections 10 of the Controller BCR**).

n) The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules. **(Section 13 of the Controller BCR).**

o) The appropriate training in data protection for personnel who have permanent or regular access to personal data**. (Section 8.2 of the Controller BCR)**.

4. The EDPB provided its opinion 30/2021 in accordance with Article 64(1)(f). The Spanish Data Protection Authority took utmost account of this opinion.

DECIDES AS FOLLOWING:

5. The Controller BCR of COLT Group provide appropriate safeguards for the transfer of personal data in accordance with Article 46(1), (2b) and Article 47 (1), (2) GDPR and hereby approves the Controller BCR of COLT Group.
6. However, before making use of the BCR it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination, including onward transfer situations. This assessment has to be conducted in order to determine if the guarantees provided by BCRs can be complied with in practice, in light of the circumstances of the possible impingement created by the third country legislation with the fundamental rights

and the circumstances surrounding the transfer. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

7. Where the data exporter in a Member State is not able to take supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCR. Therefore, the data exporter is required to suspend or end the transfer of personal data.
8. The approved BCRs will not require any specific authorization from the concerned supervisory authorities.
9. In accordance with Article 58.2.j GDPR, each concerned Supervisory Authority maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by Controller BCR of COLT GROUP are not respected.

ANNEX TO THE DECISION

The Controller BCR of COLT Group that are hereby approved cover the following:

a. Scope:
   These Binding Corporate Rules ("**Rules**") set out Colt's commitment to provide adequate protection for the transfer and processing of European Personal Data by Colt Entities acting as Data Controllers or as Data Processors when processing European Personal Data on behalf of another Colt Entity that is a Data Controller.
b. EEA countries from which transfers are to be made: Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Romania, Spain, and Sweden.
c. Third countries to which transfers are to be made: United Kingdom, Switzerland, Australia, China, Hong Kong, Japan, Korea, India, Serbia, Singapore, and United States.
d. Purposes of the transfer, categories of data subjects concerned by the transfer, categories of personal data transferred: (specified in Section 1 of the BCR);

1.1 Colt processes the following European Personal Data:

Categories of Data Subjects	**Categories of European Personal Data**
Employees, candidates, office-holders	Names, addresses, email, phone number, date of birth, ID card number, tax ID, social security number, passport number, driving license number, other

and individuals providing services to Colt as contractors	government-issued identification numbers, pension plans, marital status, number of children and family members at his/her charge, bank account, photography, benefit information, staff development records, attendance records (including any absences due to illness), salary and expenses information, disciplinary procedures, employee share holdings, financial information and creditworthiness, complete CV, education and employment history, call's records for the purpose of verifying the quality of the service and employee performance, criminal record information, drug screening information, medical history (where required for human resources administration purposes), racial and ethnic origin.
Business contacts at customers or suppliers	Name, title, contact information, such other professional Personal Data as may be required for the Relevant Group Member to conduct business with the customer or supplier as well as information regarding participation in events organised by Colt. Calls' records for the purpose of verifying the quality of the service.
Web users	IP addresses, browsing data and information about browsing preferences and habits on Colt websites.

1.2 European Personal Data are transferred to Colt Entities outside a European Country for the purposes set out below:

Where that Colt Entity manages employees, customers or suppliers	The purposes for which European Personal Data is processed are the following: • Recruitment, background screening and onboarding; • HR administration; • Employee performance management and professional development; • Payroll and administration of employee benefits; • Monitoring and whistleblowing scheme; • Research and development; • Business development; • Maintaining and building upon customer relationships; • Business planning;

	• Facilities management; • Maintaining technology infrastructure and support; • Database management; • Training; • Security, data collection and processing; • Website use information, browsing preferences and other usage information; • Fulfilling a transaction initiated by a Data Subject; • Fraud prevention or investigation, or other risk management purposes; • Identification and information verification purposes; • Protecting Colt's legal rights or assets to facilitate the acquisition or disposition of Colt businesses; • Responding to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process; • In emergencies where the health or safety of a person is endangered; and other purposes required or permitted by law or regulation.
Where that Colt Entity provides services to other Colt Entities	The purposes in this case would include hosting of European Personal Data in the course of providing IT services and security services; assisting in HR and business administration for any of the purposes above.