Colt

Binding Corporate BCR-C (Controller)

Version 2.0

CONTENTS

1. INTRODUCTION

1.1 As a global provider of telecom and data centre services, Colt understands the importance of ensuring strong safeguards in protecting Personal Data when such information is transferred and processed across borders. These Controller Binding Corporate Rules ("**BCR'C-**") set out Colt's commitment to provide adequate protection for the transfer and processing of European Personal Data by Colt Entities acting as Controllers or as Processors when processing European Personal Data on behalf of another Colt Entity that is a Controller.

1.2 These BCR-C are applicable to and are binding for each one of the Colt Entities. Colt Personnel must respect the commitments and procedures set out in these BCR-C. Failure to comply with these BCR-C may lead to disciplinary action for Personnel, up to an including dismissal.

2. SCOPE OF DATA PROCESSING AND DATA TRANSFERS

2.1 Colt processes the following European Personal Data:

Categories of Data Subjects	Categories of European Personal Data
Employees, candidates, office-holders and individuals providing services to Colt as contractors	Names, addresses, email, phone number, date of birth, ID card number, tax ID, social security number, passport number, driving license number, other 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.

2.2 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.

2.3 Most of the European Personal Data is transferred to United Kingdom, India and Japan. However, as a global group we may transfer Personal Data to other countries outside the EEA. Appendix 3 contains a list of Colt Entities, including Colt Entities which are outside a European Country.

2.4 These BCR-C are also applicable to the onward transfers of European Personal Data.

3. COLT FUNDAMENTAL PRINCIPLES

Colt's Fundamental Principles are contained within the Global Privacy Policy available on Colt's public facing website and described below:

3.1 Lawfulness, fairness and transparency

3.1.1 Colt must process European Personal Data in accordance with the following:

3.1.1.1 Lawfulness: the processing of European Personal Data must be justified on one of the lawful bases included in article 6 of the GDPR and if Sensitive Personal Data is processed, one of the

lawful bases included in article 9 of the GDPR should also apply. Most of the processing activities carried out by Colt rely on the following lawful bases:

(i) The Data Subject has given consent to the processing (e.g. in order to send marketing communications through electronic means to prospective customers).

(ii) The processing is necessary to perform a contract with the Data Subject, or to take steps at the request of the Data Subject before entering into a contract (e.g. in order to render a service).

(iii) The processing is necessary for compliance with a legal obligation to which Colt is subject (e.g. in order to provide a tax authority the information requested).

(iv) The processing is necessary for Colt's legitimate interest or those of a third party unless the interests of the Data Subject override those interests (e.g. in order to supervise employee's performance of their job).

Only process Sensitive Personal Data if, in addition, one of the following grounds for processing applies:

(i) The Data Subject has given explicit consent.

(ii) The processing is necessary to meet obligations or exercise rights in European Data Protection Law relating to employment, social security and social protection law.

(iii) The processing is necessary to establish, exercise or defend legal claims.

where applicable, the fact that Colt intends to transfer European Personal Data to the processing of European Personal Data about criminal convictions and offences will vary between jurisdictions, therefore, Colt will only transfer such European Personal Data where the processing is authorised by European Data Protection Law.

3.1.1.2 Fairness: European Personal Data must be processed fairly in ways that would be reasonably expected.

3.1.1.3 Transparency: information must be provided about the processing in a clear, precise and unambiguous way. Specifically, at the time of collecting European Personal Data, Colt will provide Data Subjects the following information:

(i) the identity and the contact details of Colt;

(ii) the contact details of the Global Data Protection Officer;

(iii) the purposes of the processing for which the European Personal Data are intended as well as the legal basis for the processing;

(iv) where the processing is based on legitimate interest, the legitimate interests pursued by Colt or by a third party;

(v) the recipients or categories of recipients of the European Personal Data, if any;

(vi) where applicable, the fact that Colt intends to transfer European Personal Data to a third country or international organisation and the existence or absence of an adequacy decision or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(vii) the period for which the European Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(viii) the existence of the right to request from Colt access to and rectification or erasure of European Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;

(ix) where the processing is based on the Data Subject's consent or explicit consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(x) the right to lodge a complaint with a supervisory authority;

(xi) whether the provision of European Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the European Personal Data and of the possible consequences of failure to provide such data;

(xii) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject; and

(xiii) the key elements of these BCR-C referred to in Section 9.3 below (this information must be provided complete and not summarized).

When European Personal Data is not obtained from the Data Subject, Colt will additionally provide the following information within a reasonable period after obtaining the European Personal Data, but at the latest within one month:

(i) the categories of European Personal Data concerned;

(ii) from which source the European Personal Data originate, and if applicable, whether it came from publicly accessible sources.

Where Colt intends to further process the European Personal Data for purposes other than the ones for which the European Personal Data were obtained, Colt shall provide the relevant Data Subjects prior to that further processing with information on those other purposes and with any other relevant information related to such further processing.

3.2 Purpose limitation

3.2.1 Colt must ensure that European Personal Data is processed only for the specific, explicit and legitimate purposes for which it was gathered and not further processed in a way which is incompatible with the purpose for collection.

3.2.2 Colt has internally implemented check points to detect the need for processing European Personal Data for any further purposes and to analyse in that case if such purposes are compatible with the original ones.

3.3 Data minimisation

3.3.1 European Personal Data collected must be adequate, relevant and be limited to the purposes for which it is processed.

3.4 Storage limitation

3.4.1 Colt must store European Personal Data allowing identification of the Data Subject for no longer than is necessary in accordance with the purpose of its collection and processing. Colt stores European Personal Data in accordance with the Colt Retention and Destruction Policy which can be found at Colt's intranet (Home > Teams > Legal and Regulatory > Data Protection > Data Privacy Policies).

3.4.2 Colt regularly reviews processing activities to check if they are aligned with the Colt Retention and Destruction Policy. Colt erases European Personal Data when no longer needed. Additionally, Colt has appropriate processes in place to comply with Data Subjects' requests for erasure of their Personal Data.

3.5 Accuracy

3.5.1 Colt must take reasonable steps to ensure that European Personal Data is accurate, complete and where necessary, kept up to date.

3.5.2 Where Colt discovers that European Personal Data is inaccurate or out of date all reasonable steps will be taken to correct or erase this data as soon as possible.

3.6 Security

3.6.1 Colt must ensure that the European Personal Data that is collected and processed is protected by implementing appropriate technical and organisational measures to prevent unauthorised or unlawful data processing, accidental loss, destruction or damage.

3.6.2 In particular, Colt must ensure that its employees who, in the performance of their duties, have access to European Personal Data, undertake to treat such

data as confidential and refrain from disclosing it to other parties, unless it is lawful to do so.

3.6.3 Where there is a suspected (or confirmed) breach of security which involves accidental, unauthorised or unlawful access to, or disclosure, alteration, loss or deletion of any European Personal Data by any Colt employee or any third party, such Colt employee or third party is required to contact the CSIRT sending an email to csirt@colt.net (available 24 hours a day, 365 days a year) in line with the Incident Response Protocol as described in Section 4.2 below.

3.7 Data protection by design and by default

3.7.1 Colt must apply measures to safeguard and demonstrate compliance with European Data Protection Law by designing and implementing data protection by design and by default:

3.7.1.1 Privacy by design: When designing a product or service, from the outset, Colt must implement appropriate technical and organisational measures which are designed to implement Colt's fundamental principles in an effective manner, as well as to integrate the necessary safeguards into the processing in order to meet the requirements of European Data Protection Law.

3.7.1.2 Privacy by default: By default, only the European Personal Data necessary to achieve each specific purpose is processed, whilst ensuring confidentiality of European Personal Data.

3.7.2 The Data Protection Impact Assessment (DPIA) is a useful tool for ensuring that privacy is built into all new processing activities and so Colt has developed guidelines and templates for:

3.7.2.1 When to conduct a DPIA (see DPIA Justification for details);

3.7.2.2 How to complete a DPIA (see DPIA Completing Guide and FAQs); and

3.7.2.3 A template DPIA document; and

3.7.2.4 A template of Artificial Intelligence DPIA applicable when the processing of European Personal Data involves the use of Artificial Intelligence tools.

3.7.3 Colt has established that a DPIA must be undertaken in the following circumstances:

3.7.3.1 Systematic and thorough evaluation of personal aspects relating to individuals, based on automated data processing, including profiling, and on which decisions about those natural persons are based.

3.7.3.2 Large-scale data processing of sensitive data or data related to criminal convictions and offences. In Colt,

large scale data processing is defined as 100 or more Data Subjects.

3.7.3.3 Systematic monitoring of a publicly accessible area.

3.7.3.4 Impact to a person's privacy is significant or maximum. Please refer to the DPIA guidance document for further examples of impact.

3.7.4 Additionally, Colt will carry out a DPIA when necessary according to European Data Protection Board (EDPB) guidelines about DPIAs and/or when necessary according to local authorities' opinions regarding data protection.

3.7.5 The Colt PIA methodology must be followed to assess and determine the privacy controls required for any business activity involving a privacy risk e.g. projects, procurement of goods and services.

3.7.6 Employees should refer to the above documentation when conducting a DPIA or assessing if one is needed and should contact the Colt Data Protection Team if required (gdpr@colt.net).

3.8 Accountability

3.8.1 Colt as a Controller is responsible for how it processes European Personal Data and complying with this policy.

3.8.2 All Employees are required to act in accordance with these BCR-C and, where appropriate, ensure that these BCR-C are enforced.

3.8.3 The Data Protection Team is responsible for these BCR-C and providing training on it, however many employees will be required to fulfil parts of these BCR-C, most notably the Individual Rights principle. Where this is the case employees must follow the procedures laid out in the principle and Individual Rights Policy.

3.8.4 Colt must maintain records of the processing activities it undertakes.

4. SECURITY

4.1 Colt Entities must implement appropriate technical and organisational measures to ensure a level of appropriate security for European Personal Data, taking into account:

4.1.1 the state of art and the costs of implementation;

4.1.2 the nature, scope, context and purposes of processing;

4.1.3 the risk of varying likelihood and severity for the rights and freedoms of natural persons; and

4.1.4 the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to European Personal Data.

By implementing said measures, Colt Entities shall have the ability to ensure confidentiality, integrity, availability and resilience of processing of European Personal Data and to restore the availability and access in the event of an incident. Moreover,

Colt Entities shall test and evaluate the effectiveness of the technical and organisational measures and the need to update the security measures implemented where necessary.

4.2 If there is a breach of security relating to European Personal Data, Colt must follow Colt's Personal Data Incident Response Process, which requires, in a manner which meets European Data Protection Law, Colt to:

4.2.1 keep records of personal data breaches affecting European Personal Data and document them comprising the facts relating to the European Personal Data breaches, its effects and the remedial action taken, making it available to the supervisory authority on request;

4.2.2 notify the Colt Lead, Global Data Protection Officer, Data Protection Director, local data protection officers and the relevant Data Protection Country Representatives, as well as to the Colt Entity acting as a Controller when another Colt Entity acting as a Processor becomes aware of a personal data breach;

4.2.3 notify without undue delay Data Subjects of personal data breaches affecting European Personal Data where the breach is likely to result in a high risk to the Data Subject; and

4.2.4 unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, notify the Competent Supervisory Authority without undue delay and not later than 72 hours or, where the Colt Entity is outside a European Country, notify the Colt Lead without undue delay which, in turn, must notify the Lead Supervisory Authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

5. SHARING PERSONAL DATA WITH THIRD PARTIES

5.1 Sharing Personal Data with Processors

5.1.1 A Colt Entity may only appoint a Processor that is not a Colt Entity to process European Personal Data where a privacy and security risk assessment has been carried out, to determine that the Processor will provide sufficient guarantees that it will implement appropriate technical and organisational measures and complies with applicable European Data Protection Laws. A Colt Entity may freely appoint another Colt Entity as a Processor.

5.1.2 The Colt Entity engaging a Processor must ensure that there is a written contract with the Processor, which is recognised as valid under European Data Protection Law, and which contains the provisions set out in Appendix 2. This is applicable irrespective of whether the Processor is a Colt Entity or not.

5.2 Sharing Personal Data with Controllers

5.2.1 A Colt Entity may share European Personal Data with another Controller where:

5.2.1.1 Colt is the Controller in respect of the European Personal Data;

5.2.1.2 it meets the Fundamental Principles set out in Colt's Global Privacy Policy, in section 3 above and the GDPR;

5.2.1.3 one of the lawful bases included in Article 6 (or 9, where applicable) of the GDPR is applicable; and

5.2.1.4 if it entails an international transfer of European Personal Data, there is a valid decision issued by the European Commission determining that the destination country, territory, or sector in a country, ensures an adequate level of protection for the European Personal Data or, in the absence of said decision, either one of the safeguards listed in Article 46 of the GDPR is in place or an exception amongst those listed in Article 49 of the GDPR is applicable.

6. TRANSFERS AND ONWARD TRANSFERS

6.1 Authorised transfers

6.1.1 European Personal Data may be shared with:

6.1.1.1 other Colt Entities bound by these BCR-C; or

6.1.1.2 entities in a European Country (as defined in these BCR-C) or located in a country or territory in respect of which there is a valid decision determining that such country, territory, or sector in a country, ensures an adequate level of protection for European Personal Data (i.e. an adequacy decision issued by the European Commission),

in accordance with these BCR-C.

6.1.2 However, Colt Entities bound by these BCR-C will use the BCR-C as a tool for transfers only where they have assessed that the law and practices in the third country of destination applicable to the processing of the Personal Data by the Colt Entity acting as Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C. To this end, Colt Entities will carry out, a transfer impact assessment as described in section 6.3 below.

6.2 Other transfers

6.2.1 In all other situations, and subject to the Colt Entity carrying out a transfer impact assessment, European Personal Data may only be shared where appropriate safeguards for the European Personal Data are put in place, as set out in Article 46 of the GDPR, such as use of standard contractual clauses adopted by the European Commission.

6.2.2 European Personal Data may also be shared, following a transfer impact assessment, in specific situations where European Data Protection Law provides a derogation to the transfer; for example, where:

6.2.2.1 the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

6.2.2.2 the transfer is necessary for the performance of a contract between the Data Subject and Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

6.2.2.3 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

6.2.2.4 the transfer is necessary for important reasons of public interest;

6.2.2.5 the transfer is necessary for the establishment, exercise or defence of legal claims.

6.3 Transfer impact assessment

6.3.1 A Colt Entity transferring European Personal Data to a non-European Country – whether to a Non-European Colt Entity or to third party Controllers or Processors located in non-European Countries – must carry out a transfer impact assessment with the help of the Data Importer if needed.

6.3.2 A transfer impact assessment must consider the following:

6.3.2.1 the specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

- purposes for which the data are transferred and processed;
- types of entities involved in the processing;
- economic sector in which the transfer or set of transfers occur;
- categories and format of the Personal Data transferred;
- location of the processing, including storage; and
- transmission channels used.

6.3.2.2 The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to

these data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards;

6.3.2.3 Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCR-C, including measures applied during the transmission and to the processing of the Personal Data in the country of destination.

6.3.3 Once assessed all the above, the transfer impact assessment will confirm that:

6.3.3.1 the level of protection required by European Data Protection Law is respected in the non-European Country concerned;

6.3.3.2 the guarantees provided by the BCR-C can be complied with in practice; and

6.3.3.3 the non-European Country legislation does not create possible interference with the fundamental rights of Data Subjects.

6.3.4 Where a transfer impact assessment cannot confirm the points set out above, the Colt Entity exporting European Personal Data will promptly inform the Colt Lead and the Colt Group Data Privacy Officer. Additionally, it should assess whether the parties to the transfer can provide supplementary measures to ensure an essentially equivalent level of protection as provided by European Data Protection Law. The Colt Lead and the Colt Group Data Privacy Officer will inform all other Colt Entities bound by these BCR-C of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Colt Entities under these BCR-C.

6.3.5 Therefore, the Colt entity exporting European Personal Data should deploy technical safeguards, as detailed below, to ensure transferred Personal Data is protected with an equivalent level of protection as provided by European Data Protection Law. Such deployment should be combined, if necessary, with contractual obligations on the importer to deploy specific security measures depending on the categories of Personal Data transferred and the country where the Personal Data is transferred, together with a regular review of the measures used, to ensure that they remain effective. The possible deployed measures and technical safeguards could be encryption, tokenisation, pseudonymisation techniques which prevent the Data Importer to be able to provide access to information which would allow the identification of individuals.

6.3.6 Where the Colt Entity exporting European Personal Data, is not able to take the 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-C. Nevertheless, if, in such case, the Colt Entity envisages to transfer Personal Data to a third country on the basis of these BCR-C, it should notify the Competent Supervisory Authority beforehand to enable that supervisory authority to ascertain

whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.

6.3.7 The Colt Entities will document appropriately the transfer impact assessment as well as the supplementary measures selected and implemented and will make such documentation available to the Competent Supervisory Authorities upon request. The Colt Entity exporting European Personal Data, will monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the third country to which the Data Exporter has transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

6.3.8 With respect to legally binding requests for disclosure of the Personal Data by a law enforcement authority or state security body, the request should be put on hold and the Competent Supervisory Authority should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the requested Colt Entity will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested Colt Entity is not in a position to notify the Competent Supervisory Authorities, it will annually provide general information on the requests it received to the Competent Supervisory Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, transfers of Personal Data by a Colt Entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

7. ACCOUNTABILITY

7.1 Colt Entities must be able to demonstrate compliance with these BCR-C.

7.2 In order to demonstrate compliance, Colt Entities must:

7.2.1 keep a record of their processing of European Personal Data, in writing, including in electronic form, which may be made available to a Competent Supervisory Authority on request, and which must include, among other information, the name and contact details for each Colt Entity, details of any transfers of European Personal Data outside a European Country and a general description of the security measures in place;

7.2.2 provide information on the categories of European Personal Data processed, the categories of Data Subject, the purposes of processing, the categories of recipients to whom European Personal Data will be disclosed and the retention periods for the European Personal Data;

7.2.3 appoint a data protection officer, if European Data Protection Law applies to the Colt Entity and if this is required by European Data Protection Law (if for

instance, the Colt Entity's core activities consist of processing of special categories of data on a large scale, or involve regular and systematic monitoring of Data Subjects on a large scale);

7.2.4 implement privacy by design and by default, by using appropriate technical and organisational measures designed to implement the Fundamental Principles and to facilitate compliance with these BCR-C in line with the Privacy by Design Policy; and

7.2.5 undertake a DPIA, before undertaking any processing of European Personal Data which is likely to result in a high risk to Data Subjects in line with the DPIA Justification. DPIAs will include a description of the processing activities and their purpose and an assessment of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect European Personal Data. Where the DPIA indicates a high and unmitigated risk, the Colt Entity must consult with the Competent Supervisory Authority or, in the case of a Non-European Colt Entity, the Colt Lead will consult with the Lead Supervisory Authority.

8. MAKING THESE BCR-C EFFECTIVE

8.1 Overseeing compliance with the BCR-C

8.1.1 Colt has designed a framework which is divided into three different levels of management and decision-making:

8.1.1.1 Top or strategic level (comprising the Global Data Protection Officer and the Global Data Protection Director: this level's duty is achieving the objectives through a general framework establishing the privacy strategy (through global policies) and the activities for the proper functioning of Colt's data protection program.

It is based on defining long-term objectives, the resources that will be used and the policies to obtain and manage such resources.

8.1.1.2 Mid or tactical level (comprising the Data Protection Team and the business units): its duties are developing detailed tasks of each area of the organisation based on the reference framework developed by the strategic level, establishing the decisions to be made, drawing up the guidelines to be used by the assigned resources, coordinating the activities carried out at the operating level and establishing a control model based on risks and controls.

The ultimate purpose is creating a top-level organisational culture regarding data protection matters which, through training and awareness, guarantees that employees know and comply with the established standards.

8.1.1.3 Lower or operating level (comprising employees and other third parties): its duties are carrying out specific tasks assigned by the other levels that every employee and contractor of the organisation must perform across all areas of work. It is developed from the alignment provided by the strategic and tactical levels. Its function is to efficiently perform routine and scheduled tasks, following the procedures and BCR-C previously defined.

8.1.2 The Global Data Protection Officer, or in his or her absence the Global Data Protection Director, is responsible for monitoring compliance with these BCR-C and can report any concerns about compliance with these BCR-C to the highest level of management at Colt.

8.1.3 The Global Data Protection Officer's role includes informing and advising Colt entities on data protection matters; involvement in DPIAs (although it is the Global Data Protection Director who is responsible for performing DPIAs); and monitoring and annually reporting on compliance with these BCR-C at a global level.

8.1.4 The Global Data Protection Officer is supported by Data Protection Country Representatives and the business units, whose role is to advise on local data protection matters, to be the primary point of contact for Data Subjects in their country; to monitor compliance and conduct training at local level and to report concerns to the Global Data Protection Officer.

8.1.5 The contact details of the Global Data Protection Officer are published in the data privacy statement available on Colt's public facing website which can be found here.

8.2 Training

8.2.1 Colt Entities must provide, on an annual basis training on these BCR-C alongside training on other privacy and data security obligations to Personnel who have permanent or regular access to European Personal Data or who have responsibility for managing processing of European Personal Data, or who are involved in the development or procurement of products, services or tools used to process European Personal Data.

8.3 Audit of the BCR-C

8.3.1 Colt's internal audit department is responsible for planning and executing privacy and data protection audits to verify compliance with these BCR-C. The members of Colt's internal audit department are guaranteed independence as to the performance of their duties related to these BCR-C audits. The Global Data Protection Officer, the Data Protection Team or any other competent function within Colt may also request *ad hoc* audits. The Data Protection Team will assist Colt's internal audit department to conduct at least one annual audit to assess compliance with these BCR-C. However, the Global Data Protection Officer will only assist Colt's internal audit department where that assistance does not result in a conflict of interest.

8.3.2 Colt Entities must ensure the audits address all aspects of these BCR-C, including Colt's security policies, IT systems, databases, if necessary, the physical record systems of Colt, provisions for sharing European Personal

Data, training, and exceptions process and set out any corrective actions required and how and when progress on corrective actions will be measured.

8.3.3 The results of the audit will be reported to the Global Data Protection Officer, the board of the Colt Lead, and to the board of Colt Technology Services Group Limited, as the ultimate parent company.

8.3.4 Colt Entities will provide copies of the results of any audit to a Competent Supervisory Authority upon request and will agree to audits by a Competent Supervisory Authority.

8.3.5 Colt Entities agree to be audited as well as inspected, including where necessary, on-site, by the competent Supervisory Authorities.

8.4 Complaints mechanism

8.4.1 Any complaints that these BCR-C may have been violated will be investigated by a person who has a suitable level of independence and impartiality.

8.4.2 If a Data Subject has a concern that a Colt Entity has processed European Personal Data relating to him or her in violation of these BCR-C, or that these BCR-C may have been violated in some other way, he or she may report this to the Human Resources Contact Centre ("**HRCC**") if they are an employee, contractor or other Personnel; the Customer Services team ("**CEST**") if they are a customer, former customer or prospect (both available here); or the Data Protection Team if they are any other individual. Complaints can also be sent by post clearly marked for the attention of the Global Data Protection Director, Colt Technology Services, Calle de Telémaco, 5, 28027 Madrid, Spain. If the complaint is considered justified either by the HRCC, the CEST or the Data Protection Team, they will as appropriate inform the Data Subject thereof and arrange for the necessary steps to be taken by the affected Colt Entity in order to correct the matter at hand and in order to implement corrective actions for the future at the affected and other Colt entities.

8.4.3 The HRCC, the CEST or the Data Protection Team (as applicable) will conclude the complaints process without undue delay and, ordinarily, within one month from the date the complaint is received. This period may be extended by two further months if this is necessary, because of the complexity of the complaint or the number of requests made by the Data Subject. The Data Subject will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

8.4.4 If the Data Subject is not satisfied with the outcome of the complaints process, has not received a reply, or where the Data Subject otherwise chooses to do so, he or she can:

8.4.4.1 raise the issue before the supervisory authority in the Member State of his or her habitual residence, place of work or the place of the alleged infringement; or

8.4.4.2 bring their claim before the competent court of the EEA Member State where Colt has an establishment or where the Data Subject has his or her habitual residence.

8.4.5 The HRCC, the CEST or the Data Protection Team (as applicable) will advise the Data Subject of these rights at the same time as telling him/ her of the outcome of the investigation.

8.4.6 The Data Protection Team keeps evidence of all the complaints received by Data Subjects through an internal data log which is kept updated and secured with restricted access.

9. RIGHTS FOR DATA SUBJECTS

9.1 Third party beneficiary rights for Data Subjects

9.1.1 Data Subjects can enforce their rights in relation to a BCR-C Breach and/or those rights, principles and duties foreseen in section 9.1.3, as 'third party beneficiaries' of these BCR-C by contacting Colt's Data Protection Team by emailing gdpr@colt.net.

9.1.2 Data Subjects also have the right to lodge a complaint with the Competent Supervisory Authority and before the competent court. In particular, Data Subjects have the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of the enforceable elements listed below.

9.1.3 Additionally, Data Subjects are able to enforce:

9.1.3.1 Third Party Beneficiary Rights as set out in section 9.1 of these BCR-C;

9.1.3.2 Fundamental Principles, lawfulness of processing, security and personal data breach notifications, restrictions on onward transfers set out in sections 3, 4 and 6 of these BCR-C;

9.1.3.3 Obligations in case of local laws and practices affecting compliance with the BCR-C and in case of government access requests as set out at section 11;

9.1.3.4 The right to complain to Colt according to section 8;

9.1.3.5 Duty to cooperate with Competent Supervisory Authorities as set out in section 10;

9.1.3.6 Liability and jurisdiction provisions as established in section 9.2;

9.1.3.7 The rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection (including, where appropriate, the right to object to be subject to decisions based solely on automated processing, including profiling), purpose limitation and data portability as established in section 9.4;

9.1.3.8 Transparency and easy access to these BCR-C as established in section 9.3.

9.1.3.9 Duty to inform the data subjects about any update of the BCR-C and of the list of BCR members as established in sections 9.3 and 13.

9.1.3.10 Right to judicial remedies, redress and compensation as established in section 9.2.

9.2 Liability, proof and jurisdiction for Data Subjects

9.2.1 If a Data Subject complains that he or she has suffered damage and can establish facts which show it is likely that the damage occurred as a result of a BCR-C Breach, then the Colt Lead must:

9.2.1.1 take necessary action to remedy the BCR-C Breach; and

9.2.1.2 compensate the Data Subject for any damages (including both financial damages and damages for non-material harm) resulting directly from the BCR-C Breach

unless the Colt Lead can show that Non-European Colt Entities are not responsible for the event giving rise to the damage, in which case it may discharge itself from any responsibility.

9.2.2 The Colt Lead accepts that the Data Subject may bring a complaint against it, to enforce his or her rights, before the supervisory authority in the Member State of his or her habitual residence, place of work or the place of the alleged infringement; or before the competent court of the EEA Member State where Colt has an establishment, or where the Data Subject has his or her habitual residence.

9.2.3 The Colt Lead accepts the liability arising from non-compliance with the BCR-C by the Non-European Colt Entities. Data Subjects will have the rights and remedies against it as if the violation had been caused by them in EEA. The Courts of an EEA Member State or another Competent Supervisory Authority will have jurisdiction over cases of non-compliance by Non-European Colt Entities.

9.2.4 While it is not required, Data Subjects are encouraged first to report their concerns directly to the relevant Colt Entity rather than a supervisory authority or court. This enables an efficient and prompt response from the relevant Colt Entity and minimizes possible delays from Competent Supervisory Authorities or court procedures. This does not prejudice Data Subjects' right to bring complaints before Competent Supervisory Authorities or courts.

9.2.5 Data Subjects may be represented by a non-profit body, organisation or association under the conditions set out in the GDPR.

9.3 Easy access to key elements of these BCR-C for Data Subjects

9.3.1 Colt must respect the Data Subjects' right to access to the key elements of these BCR-C by publishing this information on Colt's public facing website and intranet.

9.3.2 The key elements are:

9.3.2.1 the description of the material scope of the BCR-C;

9.3.2.2 the third party rights available to the Data Subjects and the means to exercise those rights;

9.3.2.3 liability for and proof relating to a BCR-C Breach;

9.3.2.4 information required by the transparency principle; and

9.3.2.5 information on Colt's Fundamental Principles and the sections on Security, Sharing Data with Third Parties and Onward Transfer.

9.3.3 Nevertheless, the whole content of these BCR-C will be available on Colt's public facing website and intranet, including Appendix 1.

9.3.4 Colt will inform Data Subjects about any update of the BCR-C and of the list of BCR members by way of publishing the new version without undue delay.

9.4 Data Subjects' rights recognised in the GDPR

9.4.1 Further to the above, Data Subjects have certain rights with regards to the processing of their Personal Data. Particularly, Data Subjects can exercise their right of access, rectification, erasure, notification regarding rectification or erasure or restriction, objection (including, where appropriate, the right to object to be subject to decisions based solely on automated processing, including profiling), restriction and portability. These rights entail the following:

9.4.1.1 Access: Data Subjects can obtain confirmation from Colt about what Personal Data is being processed and to obtain a copy of it, as contained in article 15 of the GDPR, detailed below.

a) the purposes of the processing;

b) the categories of Personal Data concerned;

c) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from Colt rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the Personal Data are not collected from the Data Subject, any available information as to their source;

h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;

i) where Personal Data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

9.4.1.2 Rectification: Data Subjects can request Colt to correct or rectify information concerning them when it is inaccurate or incomplete.

9.4.1.3 Erasure: Data Subjects can request Colt to delete their Personal Data.

9.4.1.4 Objection: Data Subjects can ask Colt to stop processing their Personal Data for certain purposes. Wen automated decisions are made by Colt, Data Subjects can specifically request not to be subject to automated decisions which produce legal effects concerning them or similarly significantly affects them.

9.4.1.5 Restriction: Data Subjects have the right to obtain from Colt restriction of processing under certain circumstances (e.g. when the Data Subject contests the accuracy of certain Personal Data, for the period during which Colt verifies the accuracy of said Personal Data).

9.4.1.6 Data portability: Data Subjects can request Colt to port their Personal Data to another organisation in a commonly-used, machine-readable format.

9.4.2 For the exercise of said rights, Data Subjects will have to follow the procedure described in Colt's individual rights privacy notice available on Colt's public facing website and, in any case, they will have to write to the Colt Entity that acts as Controller with regards to their Personal Data indicating the right exercised. The Colt Entity that acts as Controller may request a proof of identity to the Data Subject when it has reasonable doubts concerning his/her identity.

9.4.3 The Data Protection Team keeps evidence of all the requests received by Data Subjects through an internal data log which is kept updated and secured with restricted access.

10. MUTUAL ASSISTANCE AND COOPERATION WITH SUPERVISORY AUTHORITIES

10.1 Colt Entities must cooperate and assist each other, to the extent reasonably possible, to handle any matter concerning these BCR-C or the IGA, including: (1) a request, complaint or claim made by a Data Subject; or (2) an investigation or other action by a supervisory authority. The Colt Entity receiving the Data Subject request, complaint or claim is, in principle, responsible for handling any communication with the Data

Subject unless, in a specific case, the affected Colt Entities and the Data Protection Team agree otherwise (e.g. if the Colt Entity receiving the Data Subject request has no relationship with the Data Subject or if the handling procedure is centralised in a different Colt Entity).

10.2 Each Colt Entity shall provide any assistance required with any Competent Supervisory Authority and must take into account the advice from such Competent Supervisory Authority and abide the decisions, in connection with processing of European Personal Data to which these BCR-C apply.

10.3 Any dispute related to any Competent Supervisory Authority's exercise of supervision of compliance with the BCR-C will be resolved by the courts of the Member State of that Competent Supervisory Authority, in accordance with that Member State's procedural law.

11. RELATIONSHIP BETWEEN THESE BCR-C AND NATIONAL LAWS

11.1 The highest data protection standards will prevail

11.1.1 The provisions in these BCR-C are in addition to any other obligations relating to European Personal Data under applicable data protection and privacy laws. Where such laws provide a higher protection for Data Subjects, they will prevail over these BCR-C.

11.2 Laws which conflict with these BCR-C

11.2.1 If a Colt Entity considers that it is subject to laws which would prevent it from complying with these BCR-C or the IGA, or which would have a substantial effect on the protections provided by these BCR-C or the IGA, that entity must promptly inform the Colt Lead and the Colt Group Data Privacy Officer, unless this would be prohibited by a law enforcement authority or state security body, for example, where secrecy is required to preserve the confidentiality of a law enforcement investigation (a "**secrecy requirement**").

11.2.2 Where the Colt Lead considers that this matter would have a substantial adverse effect on the protections for European Personal Data provided for by these BCR-C or the IGA, it must report the matter to the Lead Supervisory Authority.

11.3 Requests from law enforcement authorities and state security bodies

11.3.1 If a Non-European Colt Entity receives a request from a law enforcement authority or state security body for disclosure of European Personal Data to which these BCR-C apply, the Colt Lead must notify its Lead Supervisory Authority. The Colt Lead should provide information about:

11.3.1.1 the European Personal Data which has been requested;

11.3.1.2 the body making the request; and

11.3.1.3 the legal basis for the request.

11.3.2 If the Colt Lead is not able to provide this information, because it is prohibited from doing so by secrecy requirements, it, or the applicable Non-European Colt Entity, must:

11.3.2.1 promptly use all best efforts to suspend the request for European Personal Data and to lift any secrecy requirements associated with the request; and

11.3.2.2 if requested by its Lead Supervisory Authority, provide information to demonstrate what actions it has taken under this section (unless this would also be prohibited by the secrecy requirements).

11.3.3 If, having used its best efforts, the Colt Lead is still not able to provide the required information to the Lead Supervisory Authority, it must provide an annual transparency report to its Lead Supervisory Authority, with general information on the requests received (such as the number of requests, the types of data and where possible the agencies making the request).

11.3.4 Colt Entities must not provide European Personal Data to law enforcement authorities or state security bodies in a way which would involve massive, disproportionate and indiscriminate transfers that go beyond what is necessary in a democratic society.

12. EXCEPTIONS

12.1 Requests for an exception from these BCR-C must be made to and authorised by the Global Data Protection Officer and, in his or her absence, the Data Protection Advisor.

12.2 Colt may deviate from these BCR-C where the deviation is lawful under European Data Protection Law of the European Country from which the European Personal Data was transferred.

13. CHANGES TO THE BCR-C AND TRANSPARENCY

13.1 Colt Entities that are signatories to the IGA agree that the Colt Lead may update these BCR-C, the IGA, and the list of Colt Entities and it shall report any changes without undue delay to the Colt Entities that are signatories of the IGA. Where a new Colt Entity is added to the list, European Personal Data must not be transferred to the new Colt Entity until the Colt Lead confirms that such entity can comply with the provisions of these BCR-C and the IGA and it is effectively bounded by these BCR-C.

13.2 The Colt Lead through the Data Protection team will:

13.2.1 maintain an up-to-date, conformed record of these BCR-C, the IGA, the list of Colt Entities subject to these BCR-C and keep track of any updates;

13.2.2 make this available to Data Subjects on request, where these BCR-C apply to their European Personal Data; and

13.2.3 inform once a year the Lead Supervisory Authority of any changes to these BCR-C and/or to the list of Colt Entities with a brief explanation of the reasons justifying said changes. The Colt Lead shall also promptly notify the Lead Supervisory Authority in the event of a change which could affect the level of protection offered by, or which would amount to a substantial change

to, these BCR-C and the IGA. The Lead Supervisory Authority should also be notified once a year in instances where no changes have been made.

14. NON-COMPLIANCE WITH THE BCR-C

14.1 If a Colt Entity acting as Data Importer is unable to comply with the BCR-C, they shall promptly inform the European Colt Entity acting as Data Exporter. In the event that the Data Importer is in breach of the BCR-C or unable to comply with the BCR-C, the Data Exporter shall suspend the transfer.

14.2 When the Data Exporter suspends the transfer, the Data Importer shall at the choice of the Data Exporter immediately return or delete the Personal Data that has been transferred under the BCR-C in its entirety where:

14.2.1 the Data Exporter has suspended the transfer and compliance with the BCR-C is not restored without undue delay and in any event within one month of suspension; or

14.2.2 the Data Importer is in substantial or persistent breach of the BCR clauses; or

14.2.3 the Data Importer fails to comply with a binding decision of a competent Court of an EEA Member or Supervisory Authority regarding its obligations under the BCR

14.3 The same shall apply to any copies of the data. The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with the BCR.-C In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with the BCR-c and will only process the data to the extent and for as long as required under that local law.

15. TERMINATION OF THE BCR-C

15.1 Should a Colt Entity acting as Data Importer ceases to be bound by the BCR-C, it may keep, return or delete the data. If the Data Importer and the Data Exporter agree that the P may be kept by the Data Importer, protection must be maintained in accordance with the GDPR.

16. ENFORCEMENT

16.1 Colt Personnel found to have violated these BCR-C will be subject to disciplinary action, up to and including dismissal. Contractors or vendors found to have violated this policy may be subject to legal action or termination of their contract or assignment.

16.2 Disciplinary action stemming from a violation of these BCR-C is determined on a case-by-case basis, taking into account all aggravating and mitigating factors. Further guidance can be found in the Disciplinary Policy. Supervisors should consult with management in their reporting line as well as Human Resources and the Data Protection Team to determine appropriate disciplinary action in a given situation.

17. CONTACT INFORMATION

17.1 Should you require any further information, or wish to see a copy of any agreement or policy referred to in these BCR-C, please contact the Data Protection Team by emailing gdpr@colt.net.

Version History			
1.0	2 August 2021	Colt Data Protection team	Approved version of BCR-C.
2.0	7 June 2024	Colt Global Data Protection Director	Update of BCR-C

Appendix 1: Glossary

BCR-C Breach: means processing of European Personal Data by a Non-European Colt Company, in breach one of the following provisions of these Binding Corporate BCR-C:

- the Fundamental Principles;
- Security (section 4);
- Sharing data with third parties (section 5);
- Onward transfer BCR-C (section 6);
- Transparency and easy access to these BCR-C ('Lawfulness, Fairness and Transparency' Fundamental Principle and section 9.3);
- Dealing with laws which conflict with this policy and requests for access to European Personal Data by law enforcement agencies and state security bodies (sections 11.2 and 11.3);
- Right to complain (section 98.44);
- Data Subjects' rights under sections 9.1 and 9.2;
- Co-operation with supervisory authorities (section 10); and
- Liability, proof & jurisdiction (section 9.2)).

Colt means Colt Technology Services Group Limited and all of its consolidated subsidiaries.

Colt Entity means a consolidated subsidiary of Colt Technology Services Group Limited which has signed the IGA.

Colt Lead means Colt Technology Services, S.A.U.

Competent Supervisory Authority means:

- the Lead Supervisory Authority; or
- any other supervisory authority which is 'concerned' by the processing of European Personal Data because:
    - a Colt Entity is established in the country or territory in which that supervisory authority is established,
    - because Data Subjects living in the country or territory of that supervisory authority are likely to be affected by a Colt Entity's processing of European Personal Data, or
    - it has received a complaint from a Data Subject relating to processing of European Personal Data by a Colt Entity.

Controller means the entity which determines the purposes and means of the processing of the Personal Data.

Data Exporter means a Colt Entity within the EEA which, both as Controller or Processor, transfers Personal Data to other Colt Entity in Third Countries.

Data Importer means a Colt Entity established in a Third Country that receives Personal Data, both as Controller or Processor, from a Colt Entity within the EEA.

Data Protection Country Representatives means the individuals in Colt who advise on local data protection matters. The Data Protection Country Representatives responsibilities are described in section 8.1.

Data Protection Team means the Global Data Protection Director, the Data Protection Country Representatives and the Global Data Protection Officer.

Data Subject means the individual to whom European Personal Data relates.

European Country means a Member State of the European Union, of the European Economic Area (i.e. Member States of the European Union and Norway, Iceland and Liechtenstein) and Switzerland (as long as an adequacy decision issued by the European Commission exists).

European Data Protection Law means:

- for European Personal Data to which the GDPR or Directive (EU) 2016/680 applies, or which have been transferred from the European Union; GDPR and any law of the European Union or of a Member State of the European Union transposing that Directive or enacting provisions associated with the GDPR or which otherwise contain BCR-C relating to the processing of Personal Data and don't contradict the GDPR or that Directive; and

- for European Personal Data to which the data protection laws of Norway, Iceland, Liechtenstein, or Switzerland apply, or which have been transferred from that country, the laws of that country

all as amended or replaced from time to time. In each case, such laws must provide appropriate safeguards for the rights and freedoms of Data Subjects.

European Economic Area or EEA means an association of European countries who have entered into a free trade agreement. This currently comprises the 27 Member States of the European Union plus Iceland, Liechtenstein and Norway.

European Personal Data means Personal Data which is processed by a Colt Entity and to which the GDPR, Directive (EU) 2016/680 or the data protection law of Norway, Iceland, Liechtenstein, Switzerland applies.

GDPR: means Regulation (EU) 2016/679.

Global Data Protection Director means the individual in Colt who oversees compliance with the BCR-C in the Global Data Protection Officer's absence.

Global Data Protection Officer means the individual in Colt responsible for monitoring compliance with the BCR-C and reporting compliance concerns to the highest level of management at Colt. The Global Data Protection Officer's responsibilities are described in section 8.1.

IGA: means the Intra Group Data Transfer Agreement which binds each Colt Entity to comply with these BCR-C.

Lead Supervisory Authority: means the Spanish Data Protection Authority.

Non-European Colt Entity: means a Colt Entity outside the European Union, Norway, Iceland, Liechtenstein, Switzerland and the United Kingdom.

Personal Data: means any information relating to an identified or identifiable, living, individual (the **'Data Subject'**).

Personnel: means an employee or office-holder of a Colt Entity, or individual providing services as a contractor to a Colt Entity, who works primarily from the premises of and has access to Colt's information technology systems.

Processor means an entity which processes Personal Data on behalf of a Controller.

Sensitive Personal Data: means Personal Data that reveal an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed to uniquely identify a natural person and data concerning health, sex life or sexual orientation.

Appendix 2: Terms to be included in contracts with Processors

Nature of processing to be described	• subject matter and duration of processing • nature and purpose of processing • type of Personal Data • categories of Data Subjects • obligations and rights of the Controller
Purpose limitation	• Processor may only process Personal Data on clear, documented instructions
Data transfer	• Processor may only transfer the data outside the EU, or, for data originating from Norway, Iceland, Liechtenstein and Switzerland, • outside that country if instructed to do so by the Controller • exception possible if the Processor is subject to European Law which requires the Personal Data to be transferred; notify the Controller of this unless that European Law imposes secrecy requirements on important public interest grounds
Confidentiality for Personnel	• All Personnel authorised to process the Personal Data to be bound by confidentiality obligations
Security	• The obligation to implement all measures required pursuant to article 32 of the GDPR and description of said measures. • The measures must be aimed at ensuring a level of security taking into consideration the state of art and the costs of implementation; the nature, scope, context and purposes of processing; the risk of varying likelihood and severity for the rights and freedoms of natural persons; and the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to European Personal Data. • The measures shall include the pseudonymisation and encryption of Personal Data and ensure the ability to ensure the confidentiality, integrity, availability and resilience of the Personal Data and must enable to restore the availability and access in the event of an incident. • The effectiveness of the technical and organisational measures must be assessed periodically and, where necessary, the security measures must be updated.
Sub-processing	• Authorisation granted by the Controller required to appoint sub-processors • If general authorisation is given, inform the Controller of changes so as to allow Controller to object (which may be met by providing a right to terminate) • Flow down substantially similar obligations to the Sub-processor. • Liability for acts of the Sub-processor
Data Subject rights	• Assist the Controller in responding to these – so far as is possible and taking into account the nature of the processing
Personal data breaches	• Assist the Controller in managing its obligations in relation to ersonal data breaches under GDPR, taking into account the nature of the processing and the information available to the Processor • Report personal data breaches to the Controller without undue delay
DPIAs	• Assist the Controller in conducing DPIAs and consulting with the Competent Supervisory Authority, taking into account the nature of the processing and the information available to the Processor

Storage limitation	• Return or delete Personal Data at the end of the services, at the Controller's choice, and delete all copies of the Personal Data • Exception possible if retention required by European Law
General assistance	• Make available all information necessary for the Controller to demonstrate it has met its obligations (under Art.28 GDPR) in appointing and managing a Processor • Notify the Controller if, in the Processor's opinion, an instruction infringes European Law
Liability	• In case the Processor infringes its obligations in relation to the processing of Personal Data, the Controller shall be able to terminate the contract
Audit	• Allow and contribute to audits, including on-site inspections, conducted by the Controller or an auditor nominated by Controller

Appendix 3: Relevant Group Companies bound by the BCR-C

Country	Entity name	Contact details	Registration Number	Tax Number
Australia	Colt Technology Services Australia Pty Ltd.	c/o Baker & McKenzie, Level 19, CBW, 181 William Street, Melbourne VIC 3000, Australia	631 678 423	ABN 29631678423
Australia	MarketPrizm B.V. (Branch)	c/o Deloitte Private, Level 1, Grovenor Place, 225 George Street, Sydney, NSW	163 287 321	ABN 17163287321
Austria	Colt Technology Services GmbH	Kärntner Ring 10-12, A-1010, Vienna	FN 175379K	ATU 45766309
Belgium	Colt Technology Services NV	Culliganlaan 2H, 1831 Diegem	VAT BE 0461.455.625 RPR Brussels	BE 0461455625
Belgium	Roosevelt Services Belgium B.V	1831 Diegem, Culliganlaan 2H Mailing address: Colt House, 20 Great Eastern Street, London, EC2A 3EH, United Kingdom	0746.874.561	
Bulgaria	Colt Technology services GmbH – Branch Bulgaria	Republic of Bulgaria, 1000 Sofia, Sredets Region, 10 Tsar Osvoboditel Blvd, 3rd floor	205565332	BG205565332
China	Colt Technology Services (China) Co., Ltd.	Office address: Room 2505, Bund Center, 222 Yanan Road East, Shanghai 200002, China Registered address: Room 108, No. 26, Jiafeng Raod, China (Shanghai) Pilot Free Trade Zone. 200131, China	913100007743162000	
China	Colt Technology Services (Dalian) Co., Ltd.	Unit 602, Building 12, No. 21 Software Park Road East, Shahekou District, Dalian, Liaoning Province	91210231MA0UM4GC5B	91210231MA0UM4GC5B
Croatia	Colt Technology Services Branch Zagreb – for telecommunication services	Nova cesta 60, Zagreb, Croatia	OIB number: 59098560040 MSB number: 081235064	HR59098560040
Czech Republic	Colt Technology Services GmbH odštěpný závod	Klimentská 1216/46, Nové Město, 110 00 Prague 1	079 32 707	CZ684737023
Denmark	Colt Technology Services A/S	Borgmester Christiansens Gade 55, 2450 Copenhagen SV	25760352	DK 25 76 03 52

Denmark	Roosevelt Services Denmark	c/o Colt Technology Services A/S, Borgmester Christiansens Gade 55, 2450 København SV Mailing address: Colt House, 20 Great Eastern Street, London, EC2A 3EH, United Kingdom	41308877	
France	Colt Technology Services SAS	23-27 rue Pierre Valette, 92240 Malakoff, France	B402 628 838	FR 404 0 262 883 8
France	Roosevelt Services France SAS	c/o Roosevelt Services France, ALAC ETOILE, 3 RUE DUE Colonel Moll, 75017 Paris, France	883 834 491	FR46883834491
Finland	Colt Technology Services Oy	Malminkatu 16 A 00100 Helsingfors	1776465-6	FI 17764656
Germany	Colt Technology Services GmbH	Gervinusstraße 18-22, 60322 Frankfurt am Main	HR-NR.: HRB46123	DE 197 498 400
Germany	RS Colocation Services Germany GmbH	Gervinusstraße 18-22, 60322 Frankfurt am Main, Germany	HRB 119195	
Hong Kong	Colt Technology Services Limited	2912-16, Tower Two, Times Square, 1 Matheson Street, Causeway Bay,Hong Kong	1860574	60966262
Hong Kong	MarketPrizm Hong Kong Ltd	2912-16, Tower Two, Times Square, 1 Matheson Street, Causeway Bay, Hong Kong	1860574	
Hungary	Colt Technology Services GmbH Hungarian Branch	1062 Budapest, Andrrassy ut 100, Hungary	01-17-001238	HU26732668
Ireland	Colt Technology Services Limited	Unit 15/16 Docklands Innovation Park, East Wall Road, Dublin 3	324439	IE 63 444 39 R
Italy	Colt Technology Services S.p.A	56, Viale Jenner Edoardo, Milan, MI 20159	12286350157	IT 122 863 501 57
India	Colt Technology Services India Pte. Limited	Unitech Business Park, Tower B, 4th & 5th Floor, South City- I, Gurgaon, 122001	U72900DL2004 PTC 125537	Gurgaon 06341824241 Bangalore 29680775929
India	Colt Network Services India Private Limited	C/o Cowrks Areocity Ground Floor & First Floor Worldmark 1, Asset Area 11, Areocity, Hospitality District, Indira Gandhi International Airport, New Delhi - 110037	U64203DL2019FTC356555	Dehli: 07AAICC4361K1ZH
Japan	MarketPrizm Japan Co. Ltd	Izumi Garden Tower 27F, 6-1 Roppongi 1-	0104-01-099717	010401099717

		chome, Minato-ku, Tokyo - From April 7, 2018		
Japan	Colt Technology Services Co., Ltd	Izumi Garden Tower 27F, 6-1 Roppongi 1-chome, Minato-ku, Tokyo	0104-01-039799	2010401039799 (JCT)
Korea	Colt Technology Services Ltd.	10FL, Kyobo Securities Building, 97 Uisadang-daero, Yeongdeungpo-gu Seoul 150-737	110114-0109733	
Luxemburg	Colt Lux Group Holding S.a r.l (LUX 3)	K2 Building, Forte 1 rue Albert Borschette 2 A 1246,Luxembourg Luxembourg	B 115940	LU 21419965
Netherlands	Colt Technology Services B.V.	Van der Madeweg 12, 1114 AM Amsterdam-Duivendrecht	33303165	NL 806825790 B 01
Netherlands	Market Prizm B.V.	20 Great Eastern Street, London, England EC2A 3EH	24295455	GB645420550
Norway	Colt Technololgy Services AS	c/o ASR Accounting AS Rakkestadveien 1, 1814 Askim	982 792 924	982792924
Poland	Colt Techonology Services GmbH (spółka z ograniczoną odpowiedzialnością) Oddział w Polsce	ul. Puławska 145, 02-715 Warsaw, Poland	KRS : 0000786057	PL1080023327
Portugal	Colt Technology Services, Unipessoal Lda	Estrada da Outurela, 118 - Parque Holanda, Edificio B1, 2790-114 Carnaxide	505289385	PT 505 289 385
Romania	Colt Technology Services RO S.R.L	50, Calea Dumbrăvii, Sibiu, Sibiu County	RO14613218	RO 14613218
Serbia	Colt Technology Services d.o.o. Beograd-Stari Grad	Kneza Mihaila street, 30, 5th Floor, Belgrade, 11000, Serbia	2 141 3011 PIB	
Singapore	Colt Technology Services Singapore Pte. Ltd.	8 Temasek Boulevard, #17-01, Suntec Tower Three, Singapore 038988	201209357C	
Singapore	MarketPrizm Singapore Pte. Ltd.	8 Marina Boulevard, #05-02, Marina Bay Financial Centre, Singapore (018981)	201321576N	201321576N
Singapore	Colt Technology Services Pte. Ltd.	8 Temasek Boulevard, #17-01, Suntec Tower Three, 038988	201003217K	201003217K

Slovakia	Colt Techonology Services GmbH, organizačná zložka Slovensko	Mudroňova 51, Bratislava – mestská časť Staré Mesto, 811 03	52 363 279	SK4120171946
Spain	Colt Technology Shared Service Centre Barcelona S.L.	Calle Acero 5-9, Barcelona	B-346885	ES B84854108
Spain	Colt Technology Services, S.A.U.	Calle Telemaco 5, 28027 Madrid Tel. +34 678 534 198	M-186178	ES A81626905
Spain	Global Rusalka S.L	C/Telémaco 5 28027 Madrid, Spain.	B88585294	ESB88585294
Sweden	Colt Technology Services AB	PO Box 3458, Luntmakargatan 18, SE-10369 Stockholm	556576-8958	SE 556 576 8958 01
Switzerland	Colt Technology Services AG	Albulastrasse 47, 8048 Zürich	CHE-106.834.429	CHE-106.834.429 MWST
Switzerland	Roosevelt Services Switzerland GmbH	c/o Schellenberg Wittmer Ltd, Lowenstrasse 19, 8001 Zurich	CHE-441.637.102	CHE-441.637.102 MWST
United Kingdom	Colt Technology Services	20 Great Eastern Street, London, England EC2A 3EH	02452736	GB 645 4205 50
United Kingdom	Colt Technology Services Europe Limited	20 Great Eastern Street, London, England EC2A 3EH	03218510	GB645420550
United Kingdom	Colt Technology Services Group Limited	20 Great Eastern Street, London, England EC2A 3EH	03232904	GB 645 4205 50
United Kingdom	Colt Group Holdings Limited	20 Great Eastern Street, London, England EC2A 3EH	11530966	
United Kingdom	Colt Pension Trustees Limited	20 Great Eastern Street, London, England EC2A 3EH	04108704	
United Kingdom	Roosevelt Services UK Limited	Colt House, 20 Great Eastern Street, London EC2A 3EH, United Kingdom	12542548	
United States	Colt Internet US Corp.	"c/o Corporation Service Company, 2711 Centerville Road, Suite 400, Wilmington, Delaware 19808 (Registered address). c/o Colt Group S.A., K2 Building, Forte 1, 2a rue Albert Borschette, L-1246 Luxembourg (Business address). 101 Hudson St, Suite 2100, Jersey City, NJ	3102974	EIN-04-3500566

		07302 (Mailing address only)		
United States	Colt Technology Services LLC	c/o The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19801 (Registered address) 141 W. Jackson Blvd., Suite 2808, Chicago, IL 60604 (Business address) 101 Hudson St, Suite 2100, Jersey City, NJ 07302 (Mailing address only)	4887258	