

Colt

Binding Corporate Rules (Processor)

Version 1.0

CONTENTS

1.	Introduction	4
2.	Scope of Data Processing and Data Transfers.....	4
3.	Colt Fundamental Principles.....	5
3.1	Lawfulness, fairness and transparency	5
3.2	Purpose limitation.....	5
3.3	Data quality	5
3.4	Security.....	5
3.5	Data Protection by design and default	6
3.6	Individual rights.....	6
4.	Security.....	6
5.	Sharing Personal Data with Third Parties.....	7
5.1	Sharing Personal Data with Sub-Processors.....	7
6.	Transfers and Onward Transfers.....	7
6.1	Authorised transfers.....	7
6.2	Other transfers	7
7.	Accountability.....	9
8.	Making these Rules Effective	10
8.1	Overseeing compliance with the Rules	10
8.2	Training.....	10
8.3	Audit of the Rules	11
8.4	Complaints mechanism.....	11
9.	Rights for Data Subjects and Customers.....	12
9.1	Third party beneficiary rights for Data Subjects.....	12
9.2	Liability, proof and jurisdiction for Data Subjects.....	14
9.3	Easy access to key elements of these Rules for Data Subjects	14
9.4	Liability and proof for Customers	15
10.	Mutual Assistance and Cooperation with Supervisory Authorities.....	16
11.	Relationship between these Rules and National Laws	16
11.1	The highest data protection standards will prevail.....	16
11.2	Laws which conflict with these Rules	16
11.3	Requests from law enforcement authorities and state security bodies	16
12.	Exceptions.....	17
13.	Changes to the Rules and Transparency.....	17
14.	Enforcement	18
15.	Contact Information	18
	Appendix 1: Glossary	20
	Appendix 2: Terms to be included in contracts with Customers and Sub-Processors.....	23
	Appendix 3: Relevant Group Companies bound by the Rules	25

1. INTRODUCTION

- 1.1 As a global provider of telecom and data centre services, Colt Technology Services ("**Colt**") understands the importance of ensuring strong safeguards in protecting Personal Data when such information is transferred and processed across borders. 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 Processors.
- 1.2 These Rules 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 Rules. Failure to comply with these Rules may lead to disciplinary action for Personnel, up to and 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
Personal Data processed on behalf of a Customer – Customer's Customers, employees or business contacts	Details of the Personal Data to be processed will be specified in the services agreement with the Customer but could include: Name, surname, date of birth, address, email, telephone number, ID card number, 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. Call's records for the purpose of verifying the quality of the service.

- 2.2 European Personal Data are transferred to Relevant Group Companies outside a European Country for the purpose set out below:

Where that Colt Entity manages employees, Customers or suppliers	The processing would include review of European Personal Data in order to: <ul style="list-style-type: none">• manage relations with Customers and suppliers• improve products and services and develop new products and services• detect or prevent fraud• conduct internal audit, compliance and risk management activities• establish, exercise or defend legal claims
Where that Colt Entity provides services to other Colt Entities as a Sub-Processor	The processing 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 Appendix 3 contains a list of Colt Entities, including details of the location of Colt Entities.

3. COLT FUNDAMENTAL PRINCIPLES

Colt's Fundamental Principles are contained within the Global Privacy Policy, save that the following principles apply where Colt is a Data Processor:

3.1 Lawfulness, fairness and transparency

- 3.1.1 Provide reasonable help and assistance to the Customer to comply with lawfulness, fairness and transparency.

3.2 Purpose limitation

- 3.2.1 Process European Personal Data only on behalf of the Customer and in compliance with the Customer's documented instructions and in accordance with the contract with the Customer. Colt entities will immediately inform the Customer if, in their opinion, an instruction infringes European Data Protection Law. Following the Customer's instructions includes:

- 3.2.1.1 giving the Customer authority to decide whether the Colt Entity can appoint a Sub-processor, as set out in Appendix 2;
- 3.2.1.2 providing the Customer with information on the main elements of the sub-processing (the parties, countries, security and onward transfer provisions, as set out in section 6 below); and
- 3.2.1.3 if requested, providing the Customer with a copy of the data protection provisions in the sub-processing contract.

- 3.2.2 At the end of provision of the services to the Customer, at the Customer's choice, Colt and sub-processors will return the European Personal Data to the Customer or delete the European Personal Data and all copies of the data and certify to the Customer that this has been done, unless legislation requires storage of the personal data transferred. In that case, Colt and sub-processors will inform the controller and warrant that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

3.3 Data quality

- 3.3.1 At the Customer's request rectify or anonymise the European Personal Data once use in identifiable form is no longer necessary and where applicable, inform any Colt Entity or Sub-Processor to whom the data have been disclosed, that this has been done.
- 3.3.2 At the Customer's request, update, correct or delete European Personal Data and, where applicable, , inform any Colt Entity or Sub-Processor to whom the data have been disclosed, that this has been done.

3.4 Security

- 3.4.1 Assist the Customer to meet its obligations for security and personal data breaches (as set out in European Data Protection Law), taking into account the nature of the processing and the information available to the Colt Entity.

3.5 Data Protection by design and default

- 3.5.1 Assist the Customer to meet its obligations for privacy by design and by default, and data protection impact assessments (as set out in European Data Protection Law), taking into account the nature of the processing and the information available to the Colt Entity.

3.6 Individual rights

- 3.6.1 At the Customer's request, execute any necessary measures (taking into account the nature of the processing and in so far as this is possible) to fulfil Customer's obligation to meet Data Subjects rights; for example, communicating useful information to help the Customer to comply. Forward any request received from a Data Subject, in respect of whom the Customer is the Data Controller, to the Customer without answering it unless a different approach is agreed with the Customer.

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 risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to European Personal Data;
 - 4.1.2 the ability to ensure confidentiality, integrity, availability and resilience of processing of European Personal Data;
 - 4.1.3 the need to test and evaluate the effectiveness of the technical and organisational measures; and
 - 4.1.4 the need to restore the availability and access to personal data
 - 4.1.5 where a Non-European Colt Entity is the Data Processor, the requirements of the European Data Protection Law which applies to the Customer and any measures specified in the service agreement with the Customer.
- 4.2 Colt entities will support the Customer when i) carrying out data protection impact assessment operations, where applicable, and ii) performing prior consultations where a data protection assessment indicates that the processing would result in a high risk pursuant to the European Data Protection Law.
- 4.3 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:
 - 4.3.1 keep records of personal data breaches affecting European Personal Data; and
 - 4.3.2 notify the Customer without undue delay, instead of notifying Data Subjects and supervisory authorities.
- 4.4 Additionally, Sub-Processors shall inform Colt (and the Customer) without undue delay after becoming aware of any personal data breach.

5. SHARING PERSONAL DATA WITH THIRD PARTIES

5.1 Sharing Personal Data with Sub-Processors

- 5.1.1 A Colt Entity may only appoint a Sub-Processor to process European Personal Data where a privacy and security risk assessment has been carried out, to determine that the Sub-Processor will provide sufficient guarantees that it will implement appropriate technical and organisational measures and complies with applicable European Data Protection Law.
- 5.1.2 The Colt Entity shall obtain the prior informed general written authorization of the Customer to appoint a Sub-Processor to process European Personal Data. The Colt Entity will provide the Customer with a comprehensive list of Sub-Processors upon Customer's request and will inform the Customer of any intended changes concerning the addition or replacement of other Sub-Processors so that the Customer has the opportunity to object to such changes, or to terminate the contract before the data are communicated to the new sub-processor.
- 5.1.3 The Colt Entity must ensure that there is a written contract with the Sub-Processor, which is recognised as valid under European Data Protection Law, and which contains the provisions set out in Appendix 2, Part B.

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 Rules; or
 - 6.1.1.2 to entities in a European Country 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 Rules, but with no further requirements to ensure adequate protection for the European Personal Data, save as to carry out, if necessary, 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 Data 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 Data 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 Data Controllers or Data Processors located in non-European Countries – must carry out a transfer impact assessment with the help of the data importer and/or the Customer if needed.
- 6.3.2 A transfer impact assessment must confirm the following:
 - 6.3.2.1 the level of protection required by European Data Protection Law is respected in the non-European Country concerned;
 - 6.3.2.2 the guarantees provided by the Rules can be complied with in practice; and
 - 6.3.2.3 the non-European Country legislation does not create possible interference with the fundamental rights of Data Subjects.
- 6.3.3 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.

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 personal data type transferred and the country of 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.

- 6.3.4 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 Rules. Nevertheless, if, in such case, the Colt Entity envisages to transfer personal data to a third country on the basis of these Rules, 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.
- 6.3.5 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.
- 6.3.6 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 Rules and make available to the Customer all information necessary to demonstrate compliance with their obligations as provided by the European Data Protection Law.
- 7.2 In order to demonstrate compliance, Colt Entities must:
- 7.2.1 allow for and contribute to audits, including inspections conducted by the Customer or another auditor mandated by the Customer as provided in their agreement with the Customer. Colt entities will immediately inform the Customer if, in their opinion, an instruction infringes European Data Protection Law;

- 7.2.2 keep a record of their processing of European Personal Data, which may be made available to a Competent Supervisory Authority on request, and which must include 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. The records shall be in writing, including in electronic form;
- 7.2.3 disclose the name and contact details of each Data Controller and its data protection officer (where one is appointed), the categories of processing carried out.;
- 7.2.4 assist the Customer to meet its obligations for privacy by design and by default, and data protection impact assessments (as set out in European Data Protection Law), taking into account the nature of the processing and the information available to the Colt Entity; and
- 7.2.5 assist the Customer in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by these Rules in practise such as data protection by design and by default.

8. MAKING THESE RULES EFFECTIVE

8.1 Overseeing compliance with the Rules

- 8.1.1 Colt has designed a framework which is divided into three different levels of management and decision-making: top or strategic level (comprising the Data Protection Officer and the Data Protection Advisor), mid or tactical level (comprising the data protection team, the local Data Protection Country Representatives and the business units) and lower or operating level (comprising employees and other third parties).
- 8.1.2 The Data Protection Officer, or in his or her absence the Data Protection Advisor, is responsible for monitoring compliance with these Rules and can report any concerns about compliance with these Rules to the highest level of management at Colt.
- 8.1.3 The Data Protection Officer's role includes informing and advising Colt entities on data protection matters; involvement in DPIAs; and monitoring and annually reporting on compliance with these at a global level.
- 8.1.4 The Data Protection Officer is supported by Data Protection Country Representatives and the business unit, 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 Data Protection Officer.

8.2 Training

- 8.2.1 Colt Entities must provide training on these Rules 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 Rules

- 8.3.1 Colt's internal audit department is responsible for planning and executing privacy and data protection audits to verify compliance with these Rules. The Data Protection team will assist Colt's internal audit department to conduct at least one annual audit to assess compliance with these Rules.
- 8.3.2 Colt Entities must ensure the audits address all aspects of these Rules, including Colt' security policies, 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 Data Protection Officer, the Colt Lead, and to Colt Technology Services Group Limited, as the ultimate parent company, and will be made accessible to Customers and to Customers' Competent Supervisory Authorities on request.
- 8.3.4 Processors and Sub-Processors will, at the request of the Customer, submit their data processing facilities for audit of the processing activities relating to that Customer which shall be carried out by the Customer or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the Customer, where applicable, in agreement with the Supervisory Authority.
- 8.3.5 Colt Entities will provide copies of the results of any audit to a Competent Supervisory Authority and will agree to audits by a Competent Supervisory Authority.

8.4 Complaints mechanism

- 8.4.1 Any complaints that these Rules 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 Rules, or that these Rules may have been violated in some other way, he or she may report this to the Customer Services team ("**CEST**") if they are the Data Subject of a Customer, former Customer or prospect; or the Data Protection team by emailing gdpr@colt.net if they are any other individual. In all and any cases any Data Subject can directly contact or involve the Global Data Protection Officer, at the following address: dpo@colt.net. The appropriate team will manage the investigation in line with the complaints procedures detailed in the Individual Rights Procedures. As outlined in the complaints procedures, a Data Subject may use various means by which to submit a complaint.
- 8.4.3 The CEST or the Data Protection team (as applicable) must forward the complaint to the Customer without undue delay for the Customer to investigate. The Data Protection team may investigate the complaint if the Customer and Colt agree to this, or if the Customer no longer exists (because it has ceased to exist in law, become insolvent or otherwise factually disappeared).
- 8.4.4 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, in which case the Data Subject will be informed accordingly.

- 8.4.5 If the Data Subject is not satisfied with the outcome of the complaints process, or where the Data Subject otherwise chooses to do so, he or she can:
 - 8.4.5.1 raise the issue before the supervisory authority in the EEA Member State of his or her habitual residence, place of work or the place of the alleged infringement; or
 - 8.4.5.2 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.
- 8.4.6 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.

9. RIGHTS FOR DATA SUBJECTS AND CUSTOMERS

9.1 Third party beneficiary rights for Data Subjects

- 9.1.1 Data Subjects can enforce their rights in relation to a BCR Breach as 'third party beneficiaries' of these Rules by contacting Colt's Data Protection team by emailing gdpr@colt.net.
- 9.1.2 Specifically, Data Subjects are able to enforce the following elements directly against Colt:
 - 9.1.2.1 Third Party Beneficiary Rights as set out in section 9.1 of these Rules;
 - 9.1.2.2 Duty to respect the instructions from the Customer regarding the data processing including for data transfers to third countries as set out at section 3.2,
 - 9.1.2.3 Duty to implement appropriate technical and organizational security measures and duty to notify any personal data breach to the Customer, as set out at section 3.4,
 - 9.1.2.4 Duty to respect the conditions when engaging a Sub-Processor either within or outside Colt, as established in section 5.1,
 - 9.1.2.5 Duty to cooperate with and assist the Customer in complying and demonstrating compliance with European Data Protection Law such as for answering requests from Data Subjects in relation to their rights, as set out at section 3.6,
 - 9.1.2.6 Easy access to BCRs as set out at section 9.3,
 - 9.1.2.7 Right to complain to Colt as set out in section 8.4,
 - 9.1.2.8 Duty to cooperate with Competent Supervisory Authorities as set out in section 10,

- 9.1.2.9 Liability, compensation and jurisdiction provisions as established in section 9.2, and
- 9.1.2.10 National legislation preventing respect of BCRs as set out in section 11.
- 9.1.3 Where the data subject is not able to bring a claim against the controller, because the data controller has factually disappeared or ceased to exist in law or has become insolvent, they shall enforce against the processor the following elements:
 - 9.1.3.1 Duty to respect these Rules by Colt entities and their employees;
 - 9.1.3.2 Liability, compensation and remediation for breaches of these Rules as established in section 9.2;
 - 9.1.3.3 Duty to prove that Colt or external Sub-Processors are not liable for any violation of the BCRs when the data subject claims damages;
 - 9.1.3.4 Easy access to BCRs as set out at section 9.3;
 - 9.1.3.5 Right to complain to Colt as set out in section 8.4,
 - 9.1.3.6 Duty to cooperate with the Customer and Competent Supervisory Authorities as set out in section 10,
 - 9.1.3.7 Duty to respect privacy principles, including the rules on transfers or onward transfers outside of the EU, as set out in sections 3 and 6;
 - 9.1.3.8 Duty to demonstrate compliance with these Rules as set out in section 7, and
 - 9.1.3.9 Duty to be transparent where national legislation prevents Colt from complying with the BCRs.
- 9.1.4 The data subjects' rights as mentioned under 9.1.2 and 9.1.3 shall cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress).

In particular, data subjects shall be entitled to lodge a complaint before the competent supervisory authority (choice between the supervisory authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence).
- 9.1.5 Where the processor and the controller involved in the same processing are found responsible for any damage caused by such processing, the data subject shall be entitled to receive compensation for the entire damage directly from the processor.

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 Breach, then the Colt Lead must:
- 9.2.1.1 take necessary action to remedy the BCR 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 Breach.
- unless the Colt Lead can show that Non-European Colt Entities or Sub-Processors are not responsible for the event giving rise to the damage and it may discharge itself from any responsibility/liability.
- 9.2.2 Where the Non-European Party was involved in the same processing as the Customer and the Colt Lead is liable for a BCR Breach in respect of that processing, then the Data Subject will be entitled to receive compensation for the entire damage directly from the Colt Lead.
- 9.2.3 The Colt Lead accepts that the Data Subject may bring a complaint against it, to enforce his or her rights, before a supervisory authority in the EEA 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. 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 Subject's right to bring complaints before Competent Supervisory Authorities or courts.

9.3 Easy access to key elements of these Rules for Data Subjects

- 9.3.1 Colt must ensure that there is easy access (for example, by publishing this information on Colt's public facing website) to key elements of these Rules for Data Subjects whose European Personal Data are processed by Non-European Colt Entities. Nevertheless, the whole content of these Rules will be available on Colt's public facing website and intranet.
- 9.3.2 The key elements are:
- 9.3.2.1 the third party rights available to the Data Subjects and the means to exercise those rights;
 - 9.3.2.2 liability for and proof relating to a BCR Breach; and
 - 9.3.2.3 information relating to:
 - (i) the duty of the Colt entities subject to these Rules and their employees to respect them (section 1.2);
 - (ii) responsibility and liability to the Customers (section 9.4);

- (iii) confirmation that the Colt Lead has sufficient assets;
- (iv) the complaints process (section 8.4 and as required from Individual Rights
- (v) Procedures);
- (vi) the duty to co-operate with Supervisory Authorities and the Customer (section 10);
- (vii) the description of the transfers, material and geographical scope of these Rules (section 2 and Appendix 2);
- (viii) the Fundamental Principles and the sections on Security, Sharing Data with Third Parties and Onward Transfer (sections 3, 4 and 6);
- (ix) the accountability provisions (section 7);
- (x) the list of entities bound by these Rules; and
- (xi) provisions on conflicts between national law and these Rules (section 11).

9.3.3 The BCRs for Processors will be incorporated into the Customer DPA by reference – a link will be available in Clause 12.2 of the Customer DPA to Colt's Privacy Portal once Colt receives approval for its relevant documentation.

9.4 Liability and proof for Customers

9.4.1 Customers can enforce relevant provisions of these Rules: the requirements set out in Appendix 2 must be included in the contract with the Customer to provide for this.

9.4.2 If a Customer can demonstrate that it has suffered damage and establish facts which show that it is likely that the damage occurred because a Non-European Party breached these Rules, or a service agreement with the Customer, while processing European Personal Data on behalf of that Customer, or due to a breach of the written agreement related to external processing by any external sub-processor established outside the EU, then the Customer may:

9.4.2.1 enforce these Rules and the service agreement against that Non-European Party; and/or

9.4.2.2 enforce these Rules and the service agreement against the Colt Lead which must also pay compensation for any damages resulting directly from the breach of these Rules or the service agreement

unless the Colt Lead can show that Non-European Party is not responsible for the breach giving rise to the damages, or that no such breach took place.

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 Rules or the IGA.
- 10.2 Each Colt Entity shall provide any assistance required by any Competent Supervisory Authority, cooperate with the Controller to the extent reasonably possible, 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 Rules and IGA apply. This obligation also applies to Sub-Processors.

11. RELATIONSHIP BETWEEN THESE RULES AND NATIONAL LAWS

11.1 The highest data protection standards will prevail

- 11.1.1 The provisions in these Rules 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 Rules.

11.2 Laws which conflict with these Rules

- 11.2.1 If a Colt Entity considers that it is subject to laws or receives instructions from the Customer, which would prevent it from complying with these Rules or the IGA, or which would have a substantial effect on the protections provided by these Rules or the IGA, that entity must promptly inform:

- 11.2.1.1 the Colt Lead and the Colt Group Data Privacy Officer; and

- 11.2.1.2 the Customer, which is entitled to suspend the transfer of data and/or terminate the contract.

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 Rules or the IGA, it must report the matter to the Lead Supervisory Authority competent for the Controller and the Supervisory Authority competent for the Processor.

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 the disclosure of European Personal Data to which these Rules apply, the Colt Lead must notify its Lead Supervisory Authority and the Customer and Customer's Competent 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 reasonable 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 taken these steps, the Colt Lead is still not able to provide the required information to the Lead Supervisory Authority or the Customer, 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 Non-European 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 Rules must be made to and authorised by the Data Protection Officer and, in his or her absence, the Data Protection Advisor.
- 12.2 Colt may deviate from these Rules 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 RULES AND TRANSPARENCY

- 13.1 Colt Entities that are signatories to the IGA agree that the Colt Lead may update these Rules, the IGA, and the list of Colt Entities and it shall report 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 Rules and the IGA and it is effectively bounded by these Rules.
- 13.2 The Colt Lead will:
 - 13.2.1 maintain an up-to-date, conformed copy of these Rules, the IGA, the list of Colt Entities and Sub-Processors subject to these Rules. The DPO of the Colt Lead will be the person in charge of complying with this obligation;
 - 13.2.2 make this record available to Data Subjects, the Customer and Supervisory Authorities on request, where these Rules apply to their European Personal Data;

13.2.3 notify the Lead Supervisory Authority once per year, or more frequently, on request of the Lead Supervisory Authority in relation to minor changes with a brief explanation of the reasons for the update, as well as:

13.2.3.1 promptly 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 Rules and the IGA; and

13.2.4 notify Customers of changes to these Rules, the IGA and the list of Colt entities subject to these Rules which are relevant to Customers and the list of Sub-processors systematically and, where a change would affect the processing conditions, provide at least thirty days advance notice to Customers, during which they have the possibility to object to the change or to terminate the contract.

14. ENFORCEMENT

14.1 Colt Personnel found to have violated these Rules will be subject to disciplinary action, up to and including dismissal. Contractors or vendors found to have violated these Rules may be subject to legal action or termination of their contract or assignment.

14.2 Disciplinary action stemming from a violation of these Rules 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.

15. CONTACT INFORMATION

15.1 Should you require any further information, or wish to see a copy of any agreement or policy referred to in these Rules, please contact the Data Protection team by emailing gdpr@colt.net

Version History			
1.0	[Date of approval]	Colt Data Protection team	Approved version of Binding Corporate Rules.

Appendix 1: Glossary

Audit Conditions means, without limiting the powers granted by European Data Protection Law to the Competent Supervisory Authorities and subject to their explicit agreement, that the person auditing will be independent and appropriately qualified, comply with Colt's security and confidentiality requirements; that the audit will be conducted during business hours; and that, unless the person responsible for the audit has reasonable grounds to believe that there is a material breach of European Data Protection Law, will take place no more than once in any year and will take place on at least thirty (30) days' notice.

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; or
- where European Personal Data is processed by a Non-European Colt Entity on behalf of a Customer, the competent supervisory authority for the Customer.

Customer/Data Controller means a person which has entered into a services agreement with a Colt Entity, where the services include the processing of European Personal Data on behalf of, and pursuant to the instructions of, the Customer, and where the Customer has authorised the transfer of European Personal Data within Colt in reliance on these Rules and the IGA.

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

Data Subject means the Data Subject 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), Switzerland (as long as an adequacy decision issued by the European Commission exists) and the United Kingdom, if an adequacy decision issued by the European Commission exists.

European Data Protection Law means:

- a. 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 rules relating to the processing of Personal Data and don't contradict the GDPR or that Directive; and
- b. for European Personal Data to which the data protection laws of Norway, Iceland, Liechtenstein, Switzerland or the United Kingdom (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 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 or the United Kingdom (applies.

GDPR: means Regulation (EU) 2016/679.

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

Lead Supervisory Authority: means the Spanish Data Protection Authority.

Non-European Party: means a Non-European Colt Entity or a Sub-Processor where section 5.1 of these Rules applies to transfers of European Personal Data to the Sub-Processor.

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.

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

- Any of the provisions in the GDPR which a Data Subject can enforce directly against a Data Processor [*duty to respect instructions; technical and organizational measures and breach reporting; provisions for appointing sub-processors; duty to co-operate with the controller; easy access; complaints; duty to co-operate with supervisory authorities; liability, compensation and jurisdiction; conflict of national law and policy; duty to prove lack of liability; respect of privacy principles and rules on transfers and onward transfers; demonstrate compliance; be transparent where national law prevents from complying*]; or
- Breach of one of the following provisions of these Binding Corporate Rules: duty to respect the BCRs; fact of third party beneficiary rights; liability and proof; easy access; complaints; duty to co-operate with authorities; privacy principles; obligation to provide a list of processor entities bound by the BCR; conflict of national law and Policy.

Relevant Group Companies: means a subsidiary of Colt Lead which has signed the IGA.

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.

Sub-Processor: means an entity appointed by a Data Processor to process European Personal Data, with the approval of the Data Controller. The entity may be Colt Lead, a Relevant Group Company or a third party Sub-Processor.

Appendix 2: Terms to be included in contracts with Customers and Sub-Processors

Topic	Requirement
PART A: TERMS TO BE INCLUDED ONLY IN CUSTOMER CONTRACTS	
BCR incorporation	<ul style="list-style-type: none"> ✓ Policy to be incorporated by reference into the agreement for services with the Customer <ul style="list-style-type: none"> ○ Does not need to include sections of the Policy which only apply where Colt is the Data Controller
Changes to Policy	<ul style="list-style-type: none"> ✓ Where Customer is notified of a significant change to the Policy and associated documents, under section 14 of the Policy, Customer to have right to terminate services affected by this
Customer to inform Data Subjects	<ul style="list-style-type: none"> ✓ If Sensitive Personal Data will be transferred, Customer must commit to inform Data Subjects that this data will be transferred to a third country ✓ Customer to inform Data Subjects that it uses Data Processors not in European Countries ✓ Customer to commit to provide a copy of these Rules (other than sections which only apply where Colt is the Data Controller) and the data protection provisions of the agreement for services between Colt and the Customer on request <ul style="list-style-type: none"> ○ Sensitive and commercially confidential information may be removed
PART B: TERMS TO BE INCLUDED IN CUSTOMER CONTRACTS AND IN CONTRACTS WITH SUB-PROCESSORS	
Nature of processing to be described	<ul style="list-style-type: none"> ✓ subject matter and duration of processing ✓ nature and purpose of processing ✓ type of Personal Data ✓ categories of Data Subjects ✓ obligations and rights of the Customer
Purpose limitation	<ul style="list-style-type: none"> ✓ only process Personal Data on clear, documented instructions ✓ If Customer is notified: <ul style="list-style-type: none"> ○ under section 11.3.1 of the Policy, that a Non-European Colt Entity has received a request to disclose Customer's European Personal Data to an overseas law enforcement agency or state security body, ○ Under section 11.2.1 of the Policy, that a Non-European Colt Entity is subject to laws which would have a substantial effect on the guarantees provided by these Rules <p>Customer may terminate the services affected by this notice</p>
Data transfer	<ul style="list-style-type: none"> ✓ only transfer the data outside the EU, or, for data originating from Norway, Iceland, Liechtenstein, Switzerland and the United Kingdom, outside that country if instructed to do so by the Customer <ul style="list-style-type: none"> ○ exception possible if Colt is subject to European Law which requires the Personal Data to be transferred; notify the Customer of this unless that European Law imposes secrecy requirements on important public interest grounds
Confidentiality for Personnel	<ul style="list-style-type: none"> ✓ All Personnel authorised to process the Personal Data to be bound by confidentiality obligations
Security	<ul style="list-style-type: none"> ✓ Description of the technical and organisational measures to protect Personal Data ✓ May be provided via link

Sub-processing	<ul style="list-style-type: none"> ✓ Customer authorisation required to appoint sub-processors, whether part of Colt or external <ul style="list-style-type: none"> ○ If general authorisation is given, inform the Customer of changes in a timely manner so as to allow Customer to object (which may be met by providing a right to terminate) ✓ Flow down substantially similar obligations to the Sub-processor. The obligations are those: <ul style="list-style-type: none"> ○ Relevant to the processing by the Sub-processor in the services agreement with the Customer ○ Set out in this Appendix 2B (including purpose limitation, acceptance of audit, duty to assist with data subject rights and queries from supervisory authorities, and with DPIAs, storage limitation, rules on appointment of sub-processors) ○ Granting Data Subjects third party beneficiary rights (Policy, section 10.1 – 10.5) ○ Duty to co-operate with supervisory authorities (Policy, section 11.2) ○ Duty to assist the Customer (Policy, section 4.3) ✓ Liability for acts of the Sub-processor
Data Subject rights	<ul style="list-style-type: none"> ✓ Assist the Customer in responding to these – so far as is possible and taking into account the nature of the processing
Personal Data breaches	<ul style="list-style-type: none"> ✓ Assist the Customer in managing its obligations in relation to Personal 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 Customer without undue delay
DPIAs	<ul style="list-style-type: none"> ✓ Assist the Customer in conducting data protection impact assessments and consulting with the competent supervisory authority, taking into account the nature of the processing and the information available to the Processor
Storage limitation	<ul style="list-style-type: none"> ✓ Return or delete Personal Data at the end of the services, at the Customer's choice, and delete all copies of the Personal Data <ul style="list-style-type: none"> ○ Exception possible if retention required by European Law
General assistance	<ul style="list-style-type: none"> ✓ Make available all information necessary for the Customer to demonstrate it has met its obligations (under Art.28 GDPR) in appointing and managing a Data Processor ✓ Notify the Customer if, in the Data Processor's opinion, an instruction infringes European Law
Audit	<ul style="list-style-type: none"> ✓ Allow and contribute to audits, including on-site inspections, conducted by the Customer or an auditor nominated by Customer <ul style="list-style-type: none"> ○ Those auditing must follow the Audit Conditions ○ Customer may select an auditor in agreement with its competent supervisory authority

Appendix 3: Relevant Group Companies bound by the Rules

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 Helsinki	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, Andrássy út 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 DCS India LLP	602, Thawar Apartment, Above Canara Bank, Main Carter Road No.5, Borivali (East) Mumbai, Maharashtra, 400066, India	AAO-6800 (LLP Identification Number)	27AAOFC4952D1ZD
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,	U64203DL2019FTC356555	Dehli: 07AAICC4361K1ZH

		Hospitality District, Indira Gandhi International Airport, New Delhi - 110037		
Japan	MarketPrizm Japan Co. Ltd	Izumi Garden Tower 27F, 6-1 Roppongi 1- chome, Minato-ku, Tokyo - From April 7, 2018	0104-01-099717	010401099717
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, Edifício 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	201321576N	201321576N

		Financial Centre, Singapore (018981)		
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 Data Centre Services UK Limited	20 Great Eastern Street, London, England EC2A 3EH	07306352	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	3102974	EIN-04-3500566

		<p>Albert Borschette, L- 1246 Luxembourg (Business address).</p> <p>101 Hudson St, Suite 2100, Jersey City, NJ 07302 (Mailing address only)</p>		
United States	Colt Technology Services LLC	<p>c/o The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19801 (Registered address)</p> <p>141 W. Jackson Blvd., Suite 2808, Chicago, IL 60604 (Business address)</p> <p>101 Hudson St, Suite 2100, Jersey City, NJ 07302 (Mailing address only)</p>	4887258	