Colt

UK Binding Corporate Rules (Controller)

Version 1.0

CONTENTS

1. Introduction 4
2. Scope of Data Processing and Data Transfers 4
3. Colt Fundamental Principles 7
   3.1 Lawfulness, fairness and transparency 7
   3.2 Purpose limitation 9
   3.3 Data minimisation 10
   3.4 Storage limitation 10
   3.5 Accuracy 10
   3.6 Security 10
   3.7 Data protection by design and by default 11
   3.8 Accountability 12
4. Security 12
5. Sharing Personal Data with Third Parties 13
   5.1 Sharing Personal Data with Data Processors 13
   5.2 Sharing Personal Data with Data Controllers 13
6. Transfers and Onward Transfers 14
   6.1 Authorised transfers 14
   6.2 Other transfers 14
7. Accountability 15
8. Making these Rules Effective 17
   8.1 Overseeing compliance with the Rules 17
   8.2 Training 18
   8.3 Audit of the Rules 18
   8.4 Complaints mechanism 18
9. Rights for Data Subjects 19
   9.1 Third party beneficiary rights for Data Subjects 19
   9.2 Liability, proof and jurisdiction for Data Subjects 20
   9.3 Easy access to key elements of these Rules for Data Subjects 21
   9.4 Data Subjects' rights recognised in the UK GDPR 21
10. Mutual Assistance and Cooperation with Supervisory Authorities 23
11. Relationship between these Rules and National Laws 23
   11.1 The highest data protection standards will prevail 23
   11.2 Laws which conflict with these Rules 23
   11.3 Requests from law enforcement authorities and state security bodies 23
12. Exceptions 24
13. Changes to the Rules and Transparency 24
14. Enforcement 25
15. Contact Information 25
Appendix 1: Glossary 27

Appendix 2: Terms to be included in contracts with Data Processors 29
Appendix 3: Relevant Group Companies bound by the Rules 31

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 UK Binding Corporate Rules ("**Rules**") set out Colt's commitment to provide adequate protection for the transfer and processing of UK Personal Data by Colt Entities acting as Data Controllers or as Data Processors when processing UK Personal Data on behalf of another Colt Entity that is a Data Controller.

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 an including dismissal.

2. SCOPE OF DATA PROCESSING AND DATA TRANSFERS

2.1 Colt processes the following UK Personal Data that are transferred to Colt Entities outside the UK for the purposes set out below:

Categories of Data Subjects	Categories of UK Personal Data	Purposes
Employees, officers, candidates	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.	• Recruitment, background screening and onboarding; • HR administration; • Employee performance management and professional development; • Payroll and administration of employee benefits; • Monitoring and whistleblowing scheme; • Training; • Security, data collection and processing; • 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. • Maintaining technology infrastructure and support; • Research and development;
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.	• Business development; • Maintaining and building upon customer relationships; • Business planning; • Facilities management; • Maintaining technology

		infrastructure and support; • Database management; • Fulfilling a transaction initiated by a Data Subject; • Fraud prevention or investigation, or other risk management purposes; • Security, data collection and processing; • 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;
Web users	IP addresses, browsing data and information about browsing preferences and habits on Colt websites.	• Website use information, browsing preferences and other usage information;

		• Security, data collection and processing; • Identification and information verification purposes; • Maintaining technology infrastructure and support; • Database management;

2.2 UK Personal Data may be transferred to the following third countries:

EMEA region	Kenya, Israel, Serbia, South Africa, Turkey
Asia-Pacific region	Australia, China, Hong Kong, India, Singapore
Americas region	USA

2.3 Appendix 3 contains a list of Colt Entities, including details of the location of Colt Entities.

2.4 These Rules are also applicable to the onward transfers of UK Personal Data between Colt Entities.

3. COLT'S FUNDAMENTAL PRINCIPLES

Colt's Fundamental Principles which all Colt Entities will abide by are contained within the Global Privacy Policy and described below:

3.1 Lawfulness, fairness and transparency

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

3.1.1.1 Lawfulness: the processing of UK Personal Data must be justified on one of the lawful bases included in article 6 of the UK GDPR and if Sensitive Personal Data is processed, one of the lawful bases included in article 9 of the UK GDPR should also apply. All 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 Data Protection Law relating to employment, social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

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

where applicable, will only transfer UK Personal Data about criminal convictions and offences where the processing is authorized by UK Data Protection Law.

3.1.1.2 Fairness: UK 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 obtaining UK 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 data protection officer;

(iii) the purposes of the processing for which the UK 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 UK Personal Data, if any;

(vi) where applicable, the fact that Colt intends to transfer 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 UK 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 UK 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 the ICO;

(xi) whether the provision of UK 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 UK 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 Rules referred to in Section 9.3 below (this information must be provided complete and not summarized).

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

(i) the categories of UK Personal Data concerned;

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

Where Colt intends to further process the UK Personal Data for purposes other than the ones for which the UK 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 UK 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 UK 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 UK 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 UK 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 UK 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 UK 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 UK Personal Data is accurate, complete and where necessary, kept up to date.

3.5.2 Where Colt discovers that UK 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 UK 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 UK 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 UK Personal Data by any Colt Personnel, such Colt Personnel 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.

3.7 Data protection by design and by default

3.7.1 Colt must apply measures to safeguard and demonstrate compliance with UK 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 UK Data Protection Law.

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

3.7.2 The Data Protection Impact Assessment (DPIA) is a useful tool for ensuring that privacy is built in to 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.

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 ICO guidelines about DPIAs.

3.7.5 The Colt DPIA 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 Data Controller is responsible for how it processes UK Personal Data and complying with this policy.

3.8.2 All Personnel are required to act in accordance with these Rules and, where appropriate, ensure that these Rules are enforced.

3.8.3 The Data Protection Team is responsible for these Rules and providing training on it, however many employees will be required to fulfil parts of these Rules, 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 UK 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 UK Personal Data.

By implementing said measures, Colt Entities shall have the ability to ensure confidentiality, integrity, availability and resilience of processing of UK 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 UK Personal Data, Colt Entities must follow Colt's Personal Data Incident Response Process, which requires, in a manner which meets UK Data Protection Law, Colt Entities to:

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

4.2.2 notify to the Global DPO, Global DPA, local DPOs and the relevant Data Protection Country Representatives;

4.2.3 notify without undue delay Data Subjects of personal data breaches affecting UK 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 ICO without undue delay and not later than 72 hours 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 Data Processors

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

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

5.2 Sharing Personal Data with Data Controllers

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

5.2.1.1 Colt is the Data Controller in respect of the UK 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 UK GDPR;

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

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

6. TRANSFERS AND ONWARD TRANSFERS

6.1 Authorised transfers

6.1.1 UK Personal Data may be shared with:

6.1.1.1 other Colt Entities bound by these Rules, in accordance with these Rules; or

6.1.1.2 other Colt Entities or third party entitieslocated in a country or territory in respect of which there is a valid decision by the UK Government determining that such country, territory, or sector in a country, ensures an adequate level of protection for UK Personal Data (i.e. an adequacy decision issued by the UK Government), in which case these Rules do not apply.

Any transfer of UK Personal Data described in this section shall be with no further requirements to ensure adequate protection for the UK Personal Data, save as to carry out, if necessary, a transfer impact assessment as described in section 6.3 below.

6.1.2 Any transfers not described in section 6.1.1 above shall meet the requirements under section 6.2 below.

6.2 Other transfers

6.2.1 In all other situations not described under section 6.1, and subject to the Colt Entity carrying out a transfer impact assessment, UK Personal Data may only be shared where appropriate safeguards for the UK Personal Data are put in place, as set out in Article 46 of the UK GDPR – except for adequacy which is covered under section 6.1.1. above-, such as use of international data transfer agreements adopted by the ICO.

6.2.2 UK Personal Data may also be shared, following a transfer impact assessment, in specific situations where UK 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 UK Personal Data to another country in respect of which there is not an adequacy decision issued by the UK Government – whether to a Colt Entity or to third party Data Controllers or Data Processors – must carry out a transfer impact assessment with the help of the data importer if needed.

6.3.2 A transfer impact assessment must confirm the following:

6.3.2.1 the level of protection required by UK Data Protection Law is respected in the country concerned;

6.3.2.2 the guarantees provided by the Rules can be complied with in practice; and

6.3.2.3 the 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 UK Personal Data will promptly inform the 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 UK Data Protection Law.

6.3.4 Therefore, the Colt entity exporting UK 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 UK 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.

6.3.5 Where the Colt Entity exporting UK Personal Data, is not able to take the supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the UK, 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 ICO beforehand to enable the ICO to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.

6.3.6 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 ICO upon request. The Colt entity exporting UK 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.

6.3.7 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 ICO 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 ICO, it will annually provide general information on the requests it received to the ICO (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.

7.2 In order to demonstrate compliance, Colt Entities must:

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

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

7.2.3 appoint a data protection officer, if UK Data Protection Law applies to the Colt Entity and if this is required by UK 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 Rules in line with the Privacy by Design Policy; and

7.2.5 undertake a DPIA, before undertaking any processing of UK Personal Data which is likely to result in a high risk to Data Subjects in line with 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 UK Personal Data. Where the DPIA indicates a high and unmitigated risk, the Colt Entity must consult with the ICO.

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:

8.1.1.1 Top or strategic level (comprising the 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 rules previously defined.

8.1.2 The Data Protection Officer, or in his or her absence the Global Data Protection Director, 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 Rules at a global level.

8.1.4 The 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 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 and/or external contractors who have permanent or regular access to UK Personal Data or who have responsibility for managing processing of UK Personal Data, or who are involved in the development or procurement of products, services or tools used to process UK 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 Global Data Protection Director 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's security policies, IT systems, databases, if necessary, the physical record systems of Colt, provisions for sharing UK 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 and the Colt Lead.

8.3.4 Colt Entities will provide copies of the results of any audit to the ICO and will agree to audits by the ICO.

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 UK 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 Human Resources Contact Centre ("**HRCC**") if they are

a member of Personnel (available at askhrcolt@neocasemail.com) and/or an external contractor; the Customer Services team ("**CEST**") if they are a customer, former customer or prospect (available at https://www.colt.net/legal/data-privacy/individual-rights/); 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: GDPR@Colt.net. The appropriate team will manage the investigation in line with the complaint procedures detailed in the Individual Rights Procedures. As outlined in the complaint procedures, a Data Subject may use various means by which to submit a complaint.

8.4.3 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.

8.4.4 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.

8.4.5 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:

8.4.5.1 raise the issue before the ICO; or

8.4.5.2 bring their claim before a competent UK court.

8.4.6 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.

8.4.7 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 Breach and/or those rights, principles and duties foreseen in section 9.1.3, as 'third party beneficiaries' of these Rules 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 ICO or a competent UK 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 Rules;

9.1.3.2 Fundamental Principles set out in section 3 of these Rules;

9.1.3.3 National legislation preventing respect of these Rules 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 the ICO 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 access, rectification, erasure, 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; and

9.1.3.8 Transparency and easy access to these Rules as established in section 9.3.

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-UK 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 ICO or before a competent UK court. While it is not required, Data Subjects are encouraged first to report their concerns directly to the relevant Colt Entity (following the procedure described in Section 8.4 above) rather than the ICO or a UK court. This enables an efficient and prompt response from the relevant Colt Entity and minimizes possible delays from the ICO or court procedures. This does not prejudice Data Subjects' right to bring complaints before the ICO or courts.

9.2.3 The Colt Lead accepts the liability arising from the non-compliance with these Rules by any Non-UK Colt Entity. Data Subjects will have the rights and remedies against it as if the violation had been caused by them in the UK. UK Courts or the ICO will have jurisdiction over cases of non-compliance by Non-UK Colt Entities.

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

9.3.1 Colt must respect the Data Subjects' right to access to the key elements of these Rules by publishing this information 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 required by the transparency principle; and

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

9.3.3 Nevertheless, the whole content of these Rules will be available on Colt's public facing website and intranet.

9.4 Data Subjects' rights recognised in the UK 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, 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 UK 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 the ICO;

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 contact the Colt Entity that acts as Data Controller with regards to their personal data (e.g. in the case of employees, the Colt Entity that that employs such employees) indicating the right exercised and will have to follow the procedure described in the relevant Colt Entity's privacy notice. The Colt Entity that acts as Data 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 THE ICO

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, including: (1) a request, complaint or claim made by a Data Subject; or (2) an investigation or other action by the ICO. 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 the ICO and must take into account the advice from the ICO and abide the decisions, in connection with processing of UK Personal Data to which these Rules apply.

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 UK 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 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 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 UK Personal Data provided for by these Rules or the IGA, it must report the matter to the ICO.

11.3 Requests from law enforcement authorities and state security bodies

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

11.3.1.1 the UK 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-UK Colt Entity, must:

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

11.3.2.2 if requested by the ICO, 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 ICO, it must provide an annual transparency report to the ICO, 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-UK Colt Entities must not provide UK 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 Global Data Protection Director.

12.2 Colt may deviate from these Rules where the deviation is lawful under UK Data Protection Law and any processing of UK Personal Data is undertaken in accordance with UK Data Protection law.

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 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, UK 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 record of these Rules, the IGA and the list of Colt Entities subject to these Rules. The Data Protection Officer of the Colt Lead will be the person in charge of complying with this obligation;

13.2.2 make this available to Data Subjects on request, where these Rules apply to their UK Personal Data; and

13.2.3 inform once a year the ICO of any changes to these Rules 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 ICO 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.

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 this policy 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 UK Binding Corporate Rules.

Appendix 1: Glossary

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

Colt Entity means any company, partnership or other entity which from time-to-time Controls, is Controlled by or is under common Control with the Colt Lead and which has signed the UK IGA. For these purposes, **Control** means the beneficial ownership of more than fifty percent (50%) of the issued share capital or the legal power to direct or cause the direction of the general management of the company, partnership or other entity in question and cognate terms shall be construed accordingly.

Colt Lead means Colt Technology Services Group Limited.

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

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

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

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

Data Protection Team means, collectively, the Global Data Protection Director, the Colt BCR Lead Data Protection Assistant, the relevant Data Protection Country Representatives and the relevant Data Protection Officer.

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

ICO means the Information Commissioner's Office, and this will be taken to mean the Information Commissioner within their formal role as the data protection authority of the United Kingdom.

Non-UK Colt Entity: means a Colt Entity outside the UK.

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

Personnel: means a Colt's employees, agents, consultants, contractors or other staff (including temporary and non-permanent staff).

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

- the Fundamental Principles;
- Security (section 4);

- Sharing data with third parties (section 5);
- Onward transfer rules (section 6);
- Transparency and easy access to these Rules ('Lawfulness, Fairness and Transparency' Fundamental Principle and section 9.3);
- Dealing with laws which conflict with this policy and requests for access to UK 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)).

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.

UK means the United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Law means the Data Protection Act 2018 and the UK GDPR 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.

UK GDPR means Regulation (EU) 2016/679 of the UK Parliament and of the Council of 27 April 2016 as it forms part of UK law by virtue of section 3 of the UK Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

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

UK Personal Data means Personal Data which is processed by a Colt Entity and to which the UK GDPR applies.

Appendix 2: Terms to be included in contracts with Data 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 Data Controller
Purpose limitation	• Data Processor may only process personal data on clear, documented instructions
Data transfer	• Data Processor may only transfer the data outside the United Kingdom if instructed to do so by the Data Controller • exception possible if the Data Processor is subject to UK Law which requires the personal data to be transferred; notify the Data Controller of this unless that UK 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 UK 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 UK 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 Data Controller required to appoint sub-processors • If general authorisation is given, inform the Data Controller of changes so as to allow Data 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 Data Controller in responding to these – so far as is possible and taking into account the nature of the processing
Personal data breaches	• Assist the Data Controller in managing its obligations in relation to personal data breaches under UK GDPR, taking into account the nature of the processing and the information available to the Processor • Report personal data breaches to the Data Controller without undue delay

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

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	Lumen Technologies Austria GmbH	Rosenbursenstraße 2/15 1010 Vienna, Austria	182735d	ATU51085301
Belgium	Lumen Technologies Belgium SA	Av. L. Grosjean 2, 1140 Evere	0462.823.523	BE0462823523
Bulgaria	Lumen Technologies Bulgaria EOOD	14 Tsar Osvoboditel Blvd, Floor 2 1000 Sofia Bulgaria	200145193	BG200145193
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	Lumen Technologies Croatia Usluge d.o.o.	Ilica 1, 10000 Zagreb, Croatia	080753908	HR50064191200
Czech Republic	CenturyLink Communications CZ s.r.o	Klimentská 1216/46 Nové Město 110 00 Praha 1 Czech Republic	271 84 099	CZ27184099
Denmark	Lumen Technologies Denmark ApS	Sydvestvej 100, 2600 Glostrup, Denmark	21264644	DK21264644
Estonia	Lumen Technologies Estonia OÜ	Lõõtsa tn 2b 11415 Tallinn Estonia	12395788	EE101606691
Finland	Lumen Technologies Finland Oy	c/o Revico Grant Thornton Oy Paciuksenkatu 27 P.O. Box 18	2346333-1	FI23463331

		00271 Helsinki		
France	Lumen Technologies France S.A.S	Le Capitole, 55 Avenue des Champs Pierreux, 92000 Nanterre, France	420 989 154 RCS NANTERRE	FR23420989154
Germany	Lumen Technologies Germany GmbH	Rüsselsheimer Straße 22, 60326 Frankfurt am Main, Germany	HRB 43850	DE195395583
Germany	Qwest Germany GmbH	Rüsselsheimer Strasse 22 Frankfurt Germany 60326	HRB 84037	DE262128381
Greece	Lumen Technologies NL B.V. Greek branch - (Lumen Technologies NL B.V. Ελληνικό Υποκατάστημα)	62 Kifissias Avenue, 15125 Maroussi, Athens - Greece	124136801001	
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	Lumen Technologies Hungary Kft	Dévai utca 26-28 1134 Budapest	01-09-879119	HU13903477
Iceland	CenturyLink Communications Iceland ehf	Suðurlandsbraut 20, 108 Reykjavík	431115-0340	121960
Ireland	CenturyLink Communications PEC Services Europe Limited	15/16 Docklands Innovation Park, East Wall, Dublin 3, Dublin, Ireland	297583	IE8297581F
Ireland	Lumen Technologies EMEA Ireland Limited	15/16 Docklands Innovation Park, East Wall, Dublin 3, Dublin, Ireland	291796	IE8297581F
Ireland	Lumen Technologies PEC Ireland Limited	Riverside One, Sir John Rogerson's Quay, Dublin 2, D02 X576	297581	IE8297581F
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, Hospitality District, Indira Gandhi International Airport, New Delhi - 110037	U64203DL2019FTC356555	Dehli: 07AAICC4361K1ZH
Israel	Lumen Technologies Israel Ltd.	7 Rival Street. Tel Aviv-Yafo 6777840 Israel	515263804	515263804
Italy	Lumen Technologies Italia Srl	Via San Giusto, 5I-20153 Milan, Italy	MI-1558220	IT12465050156
Kenya	Lumen East Africa Limited	Aln House, LR 1870/1/176, Eldama Ravine Close, Off Eldama Ravine Road, Westlands, Nairobi	CPR/2013/92036	P051423459F
Luxembourg	Lumen Technologies Luxembourg S.à r.l.	53 Boulevard Royal, L-2449 Luxembourg	B135597	LU22298540
Netherlands	CenturyLink Europe B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	34117150	NL 808121650B01
Netherlands	Level 3 Holdings B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	33299248	NL 807110978B01
Netherlands	Lumen Technologies NL B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	33299249	NL807110930B01
Netherlands	Level 3 Europe B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	34186897	NL811851084B02
Netherlands	Qwest Holdings B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	34175081	
Netherlands	Qwest Netherlands B.V.	Stekkenbergweg 4, 1105AJ Amsterdam, The Netherlands	34175082	NL8106.79.474.B.01
Norway	Lumen Technologies Norge AS	Okernveirn 121, 0579 Oslo	981 195 361	981195361MVA
Poland	Lumen Technologies Poland sp. z o.o.	Ul. Zlota 59 00-120 Warsaw Poland	0000396199	PL7010314979
Romania	Lumen Technologies Romania S.R.L.	313 - 315, Barbu Vacarescu Street, 5th floor, Bucharest, 2nd District, 020272, Romania	22164560	RO22164560
Serbia	Colt Technology Services d.o.o. Beograd-Stari Grad	Kneza Mihaila street, 30, 5th Floor, Belgrade, 11000, Serbia	2 141 3011 PIB	

Serbia	Lumen Technologies RS d.o.o. Beograd-Vračar	Krunska 73 11000 Belgrade Serbia	20924438	108057092
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	CenturyLink Communications Slovakia spol. s.r.o.	Hodžovo námestie 1A 811 06 Bratislava-Staré mesto Slovakia	36 734 349	SK2022314701
Slovenia	CenturyLink telekomunikacijske storitve d.o.o.	Bleiweisova cesta 30 1000 Ljubljana Slovenia	3896439000	SI19609710
South Africa	Group Lumen South Africa (PTY) Ltd.	Central Office Park No.4, 257 Jean Avenue, Centurion, Gauteng, 0157	2012 / 025797 / 07	4030264289
Spain	Lumen Technologies Iberia S.A.	Calle Acanto 22, 10th Floor 28045 Madrid, Spain	A82440173	ESA82440173
Sweden	CenturyLink Communications Sweden AB	Olof Palmes gata 29, 4th Floor, 111 22 Stockholm, Sweden	556624-1195	SE556624119501
Turkey	Lumen Teknoloji Hizmetleri Limited Şirketi	Küçükbakkalköy Mah. Kayışdağı Cad. Allianz Plaza No: 1 İç Kapı No: 108 Ataşehir / İstanbul	750586-0	3960630673
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	Roosevelt Services UK Limited	Colt House, 20 Great Eastern Street, London EC2A 3EH, United Kingdom	12542548	

United Kingdom	Lumen Technologies EMEA Holdings Limited	260-266 Goswell Road, London, England, EC1V 7EB	03855219	GB744433045
United Kingdom	Level 3 Communications Limited	260-266 Goswell Road, London, EC1V 7EB	03514850	GB744433045
United Kingdom	Lumen Technologies UK Limited	260-266 Goswell Road, London, EC1V 7EB	2495998	GB744433045 (EORI for Northern Ire. XI744433045000)
United Kingdom	Lumen Technologies Europe Limited	260-266 Goswell Road, London, EC1V 7EB	3728783	GB740593236
United Kingdom	Fibernet UK Limited	260-266 Goswell Road, London, EC1V 7EB	02940263	GB744433045
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 07302 (Mailing address only)	3102974	EIN-04-3500566
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	
United States	Camelot Landing, LLC	c/o Corporation Service Center, 251 Little Falls Dr., Wilmington, Delaware 19808, County of New Castle, US	7109700	