



BT Binding Corporate Rules

For the United Kingdom

Contents

1.	Introduction	3
2.	Definitions and Interpretation	3
3.	Scope	5
4.	Privacy Principles	6
5.	Accountability	8
6.	Transparency and Information Access	8
7.	Rights of Individuals	9
8.	Security and Confidentiality	10
9.	Internal Processing of Personal Data	11
10.	External Processing of Personal Data	12
11.	Assurance and Audit	13
12.	Conflicts	14
13.	Complaints	15
14.	Third Party Beneficiary Rights and Liability	16
15.	Cooperation with the Information Commissioner, Third Party Data Controllers and BT Group Companies	18
16.	New BT Group Signatories and Termination	21
17.	Variations to these Rules	21
18.	Governing Law	22
Appendix A	Participating BT Group Companies	23
Appendix B	Purposes of Processing	28
Appendix C	Security and Organisational Measures	35
Appendix D	Agreement of Adherence	38
Appendix E	General Processor Requirements	39
Appendix F	Revision Control History	40

THIS AGREEMENT is made between the BT Group Companies.

1. Introduction

- 1.1 These Rules apply to the processing of Personal Data by BT Group Companies and will provide adequate protection for the transfer of Personal Data outside of the UK and Approved Countries in accordance with the requirements of the UK Data Protection Legislation, as set out in more detail in paragraph 3.
- 1.2 The Board of Directors of each of the BT Group Companies (the **"Board of Directors"**) are committed to ensuring compliance with these Rules.
- 1.3 All Personnel of each BT Group Company will: (i) have a copy of these Rules made available to them; (ii) be provided with appropriate training on compliance with these Rules; and (iii) be required to ensure compliance with these Rules by agreeing to comply with the "BT Being Trusted: Our Code", which makes reference to these Rules and contains sanctions in the event of non-compliance.
- 1.4 All Personnel of each BT Data Processor and BT Sub-Processor will respect: (i) the relevant Third Party Data Controller's instructions in relation to the processing of its Third Party Personal Data, and (ii) security and confidentiality measures as set out in the relevant Data Processing Agreement.
- 1.5 The person that is ultimately responsible for compliance with these Rules is: the BT Group Data Protection & Ethics Officer (the **"Group DPO"**).
- 1.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999, these Rules are not intended to, and do not, give any person who is not a BT Group Company any rights to enforce any provisions contained in it, except any provision which expressly provides for enforcement by any other third party which shall be enforceable with its express terms (which for the avoidance of doubt shall include the third party beneficiary rights of Individuals as set out in paragraph 14 and Third Party Data Controllers).
- 1.7 These Rules are legally binding and shall apply to and be enforced by every BT Group Company that is a party to them, and by Personnel. Each BT Group Company shall ensure that its Personnel comply with these Rules, and failure to do so may result in disciplinary action in the case of employees, or other contractual consequences in the case of other Personnel, in accordance with BT Being Trusted: Our Code and applicable contractual terms.
- 1.8 In consideration of the mutual promises, undertakings, and obligations set out in this Agreement, including the benefit to each BT Group Company of being able to make and receive international transfers of Personal Data in a manner compliant with UK Data Protection Legislation, the Parties agree to be legally bound by the terms contained herein.

2. Definitions and Interpretation

- 2.1 In these Rules: **"controller"**, **"processor"**, **"data subject"**, **"personal data"**, **"processing"** and **"special categories of personal data"** shall each have the same meanings as are given to them in the UK Data Protection Legislation and **"process"** and **"processed"** shall be construed accordingly.

- 2.2 In these Rules, the following terms have the meanings set out below:

"Agreement of Adherence" means an Agreement of adherence with British Telecommunications Limited (BT Ltd) substantially in the form set out in Appendix D (Agreement of Adherence);

"Applicable Law" means the mandatory requirements of any law, enactment, regulation, regulatory policy, guideline from a relevant and competent regulatory authority applicable to a BT Group Company and/or to any of the activities of a BT Group Company, including but not limited to UK Data Protection Legislation;

"Approved Country" means any country outside of the UK recognised by the UK Government as ensuring an adequate level of protection for personal data;

"Board of Directors" has the meaning provided in paragraph 1.2;

"BT" means the BT Group Companies (including BT Ltd) and their successors and assigns;

"BT Being Trusted: Our Code" means BT's overarching statement of business principles which is available to all Personnel <https://intra.bt.com/bt/ourcode/Pages/index.aspx>, as amended or replaced from time to time;

"BT Data Controller" means the relevant BT Group Company acting as a controller of Personal Data;

"BT Data Processor" means any BT Group Company acting as a processor on behalf of a BT Data Controller or a Third Party Data Controller (as the context requires);

"BT Privacy Office" has the meaning provided in paragraph 11;

"BT Group Companies" means the entities set out in Appendix A (Participating BT Group Companies) comprising all BT operating entities which have executed these Rules (or an Agreement of Adherence in accordance with paragraph 16 (*New BT Group Signatories*)) and are bound by these Rules;

"BT Personal Data" means personal data (other than Third Party Personal Data) to which the UK Data Protection Legislation applies, originating from or processed by and on behalf of any BT Group Company;

"BT Ltd" means British Telecommunications Limited a company registered in England and Wales under company number 1800000 whose registered office is at: 1 Braham Street, London, United Kingdom, E1 8EE, and its successors and assigns;

"BT Sub-Processor" means any BT Group Company sub-processor that processes Personal Data), under an agreement or arrangement with a BT Data Processor, for the purposes of providing processing services to a Data Controller;

"Data Controller" means a BT Data Controller and/or a Third Party Data Controller (as the context requires).

"Data Exporter" means a BT Data Controller or where permitted a BT Data Processor established in an Approved Country that transfers Personal Data to a Data Importer.

"Data Importer" means a BT Data Controller or BT Data Processor located in a third country that receives Personal Data from the Data Exporter.

"Data Processing Agreement(s)" means any contract or clauses within a contract in respect of Third Party Personal Data between the relevant Third Party Data Controller and the relevant BT Data Processor, which meets the requirements of Art 28(3) of the UK GDPR and otherwise requires BT to comply with these Rules;

"Group DPO" has the meaning provided in paragraph 1.5;

"Individual" shall have the same meaning as data subject under UK Data Protection Legislation;

"Personal Data" means Third Party Personal Data and/or BT Personal Data (as the context requires);

"Personal Data Breach" has the meaning provided in paragraph 8.3;

"Personnel" means all BT personnel (including any contractor, staff or employee as defined in Appendix B) that have permanent or regular access to Personal Data; and/or are involved in the collection of such Personal Data; and/or are involved in the development of tools using such Personal Data;

"Responsible BT Group Company" has the meaning provided in paragraph 14.1;

"Rules" means the rights and obligations set out in this agreement and its appendices;

"Sub-Processing Agreement" means a sub-processing agreement between a BT Data Processor and a BT Sub-Processor or external sub-processor (as the context requires) entered into for the purposes of providing processing services to a Data Controller;

"Third Party Data Controller" means the relevant third party acting as a data controller of Third Party Personal Data (which controller has entered into a Data Processing Agreement with a BT Data Processor);

“Third Party Personal Data” means personal data originating from a Third Party Data Controller to which the UK Data Protection Legislation applies, that is subsequently disclosed or made available to a BT Data Processor;

“Third Party Personal Data Breach” has the meaning given to it in paragraph 8.5;

“UK” means the United Kingdom of Great Britain and Northern Ireland;

“UK Data Protection Legislation” means any law relating to privacy and data protection applicable in England, Wales, Scotland and Northern Ireland, including the UK GDPR and the Data Protection Act 2018 and any amendments to or replacements for such laws;

“UK GDPR” means the General Data Protection Regulation EU 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended);

“UK Standard Contractual Clauses” means the International Data Transfer Addendum to the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022.

“Working Day” means a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

2.3 These Rules will be interpreted in accordance with the UK Data Protection Legislation.

2.4 When used in these Rules, the term “non-material damage” shall be interpreted (i) in the same manner as the term set out in the UK GDPR, and (ii) without prejudice to the ordinary rules of causation and remoteness under the governing law of these Rules.

2.5 In these Rules:

2.5.1 references to a statute or statutory provision include:

- (a) that statute or statutory provision as from time to time modified, re-enacted, consolidated, or replaced, whether before or after the date of these Rules, which in the case of the UK GDPR shall include (without limitation) any relevant delegated or implementing acts as modified, re-enacted, consolidated, or replaced from time to time;
- (b) any past statute or statutory provision (as from time to time modified, re-enacted or consolidated) which that statute or provision has directly or indirectly replaced; and
- (c) any subordinate legislation made from time to time under that statute or statutory provision, which is in force at the date of these Rules;

2.5.2 references to:

- (a) a person includes any company, partnership or unincorporated association (whether or not having separate legal personality); and
- (b) a company include any company, corporation or anybody corporate, wherever incorporated; and

2.5.3 references to one gender include all genders and references to the singular include the plural and vice versa.

3. Scope

3.1 These Rules apply to all Personal Data (that falls within the geographical scope set out in paragraph 3.2) which is processed by BT Group Companies, whether acting as a controller, processor, or Sub-Processor. These Rules are the appropriate safeguard for transfers of personal data out of the UK to members located in countries not subject to a UK adequacy decision. The Rules do not apply where a transfer is otherwise

lawfully permitted by UK Data Protection Legislation, such as where it is made to a country covered by an adequacy decision.

3.2 These Rules apply to:

- 3.2.1 the processing of Personal Data in the UK by a BT Group Company located in the UK;
- 3.2.2 the processing of Personal Data by a BT Group Company located outside of the UK (including where such Personal Data has been transferred directly to a BT Group Company by or on behalf of a Third Party Data Controller);
- 3.2.3 any transfer of Personal Data out of the UK by one BT Group Company to another BT Group Company except when otherwise allowed by UK Data Protection Legislation; and
- 3.2.4 any subsequent processing or sub-processing of the Personal Data described in paragraph 3.2.3 by a BT Group Company located outside of the UK including any transfer from one non-UK based BT Group Company to another non-UK based BT Group Company (except when otherwise allowed under UK Data Protection Legislation).

3.3 These Rules cover the processing of Personal Data both automated or structured, whether on-line and off-line (provided that in the case of off-line records, the Personal Data forms part of a structured manual filing system), and does not apply to manual unstructured processing of Personal Data.

3.4 A list of the BT Group Companies which are bound by these Rules can be found in Appendix A (BT Group Companies). The Group DPO ensures this list shall be updated from time to time to reflect new BT Group Companies that have become bound by these Rules or BT Group Companies that have ceased to be bound by these Rules.

3.5 The nature and material scope of the Personal Data that the BT Group Companies process (as part of their regular business activities) is set out in Appendix B (Purposes of Processing). All of the data processing set out in Appendix B (Purposes of Processing) is conducted by BT Data Controllers. Where required by a Third Party Data Controller, some of these activities marked by an asterisk (or others specified in a Data Processing Agreement) may be carried out by a BT Data Processor.

4. Privacy Principles

4.1 When acting as a BT Data Controller, each BT Group Company will follow the principles set out in paragraph 4.2 (subject to exemptions provided by UK Data Protection Legislation) when processing Personal Data:

4.2 Personal Data will be:

- 4.2.1 processed fairly, lawfully, and in a transparent manner in relation to the Individual, subject to the security measures set out in paragraph 8.2. All processing will be based on a valid lawful basis under Article 6 of the UK GDPR, which may include, depending on the specific processing activity:
 - (a) the consent of the Individual;
 - (b) the performance of a contract to which the Individual is a party or to take steps at the request of the Individual prior to entering into a contract;
 - (c) compliance with a legal obligation to which a BT Group Company is subject;
 - (d) the protection of the vital interests of the Individual or of another natural person;
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in BT Group Company; or
 - (f) the legitimate interests pursued by a BT Group Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Individual.

- 4.2.2 collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
- 4.2.3 only processed to the extent that it is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- 4.2.4 accurate and, where necessary, kept up to date and every reasonable step will be taken to ensure that Personal Data, which is inaccurate or incomplete, taking into account the purposes for which it was collected or for which it is further processed, is erased or corrected without delay;
- 4.2.5 kept in a form which permits identification of Individuals for no longer than is necessary for the purposes for which the Personal Data was collected or is further processed;
- 4.2.6 in some cases, special categories of personal data are processed. Such data is subject to additional protection and controls consistent with UK Data Protection Legislation and will only be processed where a valid condition under Article 9 of the UK GDPR applies. Depending on the specific processing activity, this may include:
 - (a) the explicit consent of the Individual;
 - (b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
 - (c) the processing is necessary to protect the vital interests of the Individual or of another natural person where the Individual is physically or legally incapable of giving consent;
 - (d) the processing is necessary for the establishment, exercise or defence of legal claims; or
 - (e) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
- 4.2.7 BT processes special category data (Article 9 UK GDPR) and criminal offence data (Article 10 UK GDPR) only where legally permitted and necessary. This includes processing under:
 - (a) Article 9 conditions (as listed in clause 4.2.6 above);
 - (b) Article 10 requirements with appropriate UK law authorisation and safeguards; and
 - (c) Schedule 1 DPA 2018 conditions including employment purposes, statutory requirements, equality monitoring, fraud prevention, and other substantial public interest grounds.
- 4.3 When acting as a BT Data Processor or BT Sub-Processor for a Third Party Data Controller, each BT Group Company will comply with the following principles (subject to exemptions provided by UK Data Protection Legislation) when processing Third Party Personal Data:
 - 4.3.1 help and assist the Third Party Data Controller to comply with the legal requirement in Article 5(1)(a) of the UK GDPR to process Third Party Personal Data fairly, lawfully and in a transparent manner;
 - 4.3.2 process Third Party Personal Data in compliance with the Third Party Data Controller's documented instructions, including with regard to transfers of Personal Data outside of the UK to a non-Approved Country, unless required otherwise by applicable UK law to which the BT Data Processor is subject. In such a case, the BT Data Processor (as informed by the BT Sub-Processor, as the case may be) will inform the Third Party Data Controller of that legal requirement before the processing takes place unless prohibited from doing so by that UK law on important grounds of public interest. In all other cases, if the BT Data Processor cannot provide such compliance for whatever reasons, it agrees to promptly inform the Third Party Data Controller of its inability to comply, in which case the Third Party Data Controller may be entitled to suspend the transfer of data and/or terminate the relevant Data Processing Agreement, subject to the terms and conditions of the relevant Data Processing Agreement.

- 4.3.3 in the event of expiry or the termination of data processing services provided on behalf of a Third Party Data Controller, at the option of the Third Party Data Controller, return all relevant Third Party Personal Data (including copies) to the third party Data Controller, or destroy this Third Party Personal Data and certify to the Third Party Data Controller that they have done so, unless Applicable Law prevents them from returning or destroying the Third Party Personal Data, in which case the relevant BT Data Processor and/or BT Sub-Processor will inform the Third Party Data Controller and warrant to it that they will guarantee the confidentiality of this Third Party Personal Data and that they will no longer actively process this Third Party Personal Data; and
- 4.3.4 to the extent relevant to the services provided under the agreement with the Third Party Data Controller, provide reasonable assistance to such Third Party Data Controller to comply with the legal requirements in relation to data quality, as set out in the Articles 5(1)(b)-(e) of the UK GDPR. Specifically, they will:
- (a) introduce any necessary measures when reasonably requested by the Third Party Data Controller, in order to have relevant Third Party Personal Data processed by the BT Data Processor and/or BT Sub-Processor updated, corrected or deleted and inform other BT Group Companies to which the Third Party Personal Data has been disclosed of these updates, corrections or deletions; and
 - (b) introduce any necessary measures when reasonably requested by the Third Party Data Controller, in order to have relevant Third Party Personal Data processed by the BT Data Processor and/or BT Sub-Processor deleted or anonymised once it is no longer necessary to identify Individuals and inform other BT Group Companies to which the Third Party Personal Data has been disclosed of any deletion or anonymisation.

5. Accountability

- 5.1 Each BT Group Company acting as a BT Data Controller shall be responsible for, and must be able to demonstrate, compliance with the principles and obligations set out in these Rules and the UK Data Protection Legislation, in accordance with the accountability principle under Article 5(2) of the UK GDPR.
- 5.2 All BT Data Controllers and BT Data Processors will maintain a record of all categories of processing activities they carry out, in line with Article 30 of the UK GDPR, to demonstrate compliance with the requirements set up by these Rules, including the principles set out at paragraph 4.2 above. This record shall be made available to the Information Commissioner upon request.
- 5.3 BT Data Controllers will carry out data protection impact assessments where they identify that processing is likely to result in a high risk to the rights and freedoms of Individuals. Where a data protection impact assessment indicates that the processing would result in a high risk to Individuals in the absence of measures taken by the BT Data Controller to mitigate that risk, the BT Data Controller will consult with the Information Commissioner prior to commencing the processing.
- 5.4 BT Data Controllers shall comply with their obligations in respect of data protection by design and default in line with Article 25 of the UK GDPR, to facilitate compliance with the requirements set out by these Rules in practice.

6. Transparency and Information Access

- 6.1 All BT Group Companies will make sure that these Rules are readily available to Individuals. The Rules are published on BT's website, along with BT's Privacy Policy and can be accessed at www.bt.com/privacy-policy. BT employees can find information about the Rules on BT's intranet.
- 6.2 Individuals can contact BT if they have any queries in relation to the handling of their Personal Data under these Rules, or if they would like to obtain a hard-copy version of these Rules. Please contact us using [this form](#), or our BT Privacy Office contact details are:

Data Privacy Team, BT
Floor 16
1 Braham Street
London
EI 8EE

- 6.3 Each BT Data Controller will inform Individuals of the processing of their Personal Data through privacy notices provided by the relevant BT Group Companies and other relevant means
- 6.4 Before any BT Data Controller, will process any Personal Data, it will make sure that Individuals have been provided with the following information:
- 6.4.1 the identity and contact details of the BT Data Controller (and of their representatives and data protection officers, if any);
 - 6.4.2 the purposes for which the Personal Data is intended to be processed, the legal basis for the processing and, where the processing is based on legitimate interests, the details of such interests;
 - 6.4.3 the recipients or categories of recipients of the Personal Data;
 - 6.4.4 details of any intended transfers of Personal Data outside of the UK, the safeguards relied upon (such as these Rules) and the means to obtain copies of any relevant transfer agreements;
 - 6.4.5 how long the BT Group Company will store the Personal Data, or the criteria used to define the period;
 - 6.4.6 details of the Individual's right to access Personal Data held about them, to require the correction or erasure of their Personal Data, to object to or restrict processing of their Personal Data and the right to data portability;
 - 6.4.7 the Individual's right to complain to the Information Commissioner;
 - 6.4.8 whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, whether the Individual is obliged to provide their Personal Data and of the possible consequences of failure to provide such Personal Data;
 - 6.4.9 the Individual's right to withdraw their consent at any time when that BT Group Company is relying on such consent to process the Individual's Personal Data;
 - 6.4.10 the reasoning for any automated decisions (as well as the significance and the envisaged consequences of such processing), where the BT Group Company takes decisions about Individuals using solely automated processes, and those decisions significantly affect an Individual or produce legal effects concerning an Individual; and
 - 6.4.11 the source from which the BT Group Company received the Personal Data and the categories of Personal Data processed, where it was not collected from the Individual themselves.
- 6.5 Where the Personal Data has not been collected directly from the Individual, the obligation to give Individuals the information set out in paragraph 6.4 will not apply if the provision of such information: proves impossible, would involve a disproportionate effort, or if recording or disclosure is expressly permitted by Applicable Law.

7. Rights of Individuals

- 7.1 Subject to exemptions, limitation and scope of application provided by UK Data Protection Legislation, each BT Data Controller will, make sure that every Individual has the right to:
- 7.1.1 obtain free of charge a copy of their Personal Data that is processed by the BT Group Company; such right being, in any event, subject to UK Data Protection Legislation.
 - 7.1.2 obtain the correction, erasure or restriction of their Personal Data that is processed by the BT Group Company;
 - 7.1.3 object, at any time on grounds relating to their particular situation, to the processing of their Personal Data which is based on point (e) or (f) of Article 6(1) of the UK GDPR, including profiling based on those provisions. The BT Data Controller shall no longer process the Personal Data, unless it demonstrates compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the Individual or for the establishment, exercise or defence of legal claims;

- 7.1.4 object, on request and free of charge, to the processing of their Personal Data for the purposes of direct marketing;
- 7.1.5 (where relevant) not be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning him or her or significantly affects him or her; and/or
- 7.1.6 data portability, in a structured, commonly used machine-readable format.
- 7.2 In the event that an Individual makes a request for their Personal Data in accordance with paragraph 7.1.1 above the relevant BT Group Company will respond to any such request and provide the requested information (unless it is permitted by UK Data Protection Legislation to refuse the request, or to comply only in part with the request, or in the case of Third Party Personal Data, unless otherwise agreed with the Third Party Data Controller) within the timescales set by UK Data Protection Legislation. All requests in respect of an Individual's Personal Data should be made to [BT | Individual Rights Request form](#), or alternatively addressed to:
- Data Privacy Team, BT
Floor 16
1 Braham Street
London
E1 8EE
- 7.3 Each BT Data Controller will make sure that no evaluation or decision about an Individual which significantly affects that Individual will be based only on the automated processing of their Personal Data unless the evaluation or decision:
- 7.3.1 is taken during the entering into or performance of a contract, at the request of the Individual; or
- 7.3.2 is allowed by Applicable Law which also contains measures to protect the Individual's legitimate interests; or
- 7.3.3 is based on the Individual's explicit consent.
- 7.4 Where the decision is based on 7.3.1 or 7.3.3, the BT Data Controller shall implement suitable measures to safeguard the Individual's rights, freedoms and legitimate interest including informing the Individual about the automated processing and any logic involved as well as any significant consequences for the Individual as well as providing the right to obtain human intervention and to challenge the decision
- 7.5 Each BT Data Processor and BT Sub-Processor will, in respect of Third Party Personal Data:
- 7.5.1 to the extent relevant, and insofar as possible, at the Third Party Data Controller's reasonable request, assist the Third Party Data Controller with the fulfilment of the Third Party Data Controller's obligations to respond to requests for exercising the Individual's rights as set out in Art 28(3)(e) of the UK GDPR and communicate useful information of which it is aware to help the Third Party Data Controller to comply with the duty to respect the rights of Individuals; and
- 7.5.2 send to the Third Party Data Controller any Individual request without answering it, unless authorised to do so.
- 7.6 Where a BT Data Controller has rectified or erased personal data or restricted its processing in accordance with this Clause 7, it shall communicate such action to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort, in accordance with its obligation under Article 19 of the UK GDPR. The BT Data Controller shall also inform the Individual about those recipients (or where providing specific recipients proves impossible or involves disproportionate effort, the categories of recipients) if the Individual requests it.

8. Security and Confidentiality

- 8.1 All BT Group Companies will take appropriate technical and organisational security measures to ensure a level of security appropriate to the risks presented by the processing of Personal Data.
- 8.2 In determining the technical and organisational security measures, consideration will be given to the technological developments (state of the art), the cost of their implementation and the nature, scope and

purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of Individuals posed by BT's processing of Personal Data.

- 8.3 Any BT Group Company that becomes aware of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data ("**Personal Data Breach**") will report such Personal Data Breach to the Group DPO and Responsible BT Group Company without undue delay, providing details of the facts relating to the Personal Data Breach, its effects and the remedial action taken. If the Group DPO determines that the security breach is likely to result in:
- 8.3.1 a risk to the rights and freedoms of individuals, then the Information Commissioner will be informed without undue delay and, where feasible, not later than 72 hours after the relevant BT Group Company became aware of the Personal Data Breach; or
 - 8.3.2 a high risk to the rights and freedoms of individuals, then in addition to informing the Information Commissioner in accordance with paragraph 8.3.1, affected Individuals will also be informed of the Personal Data Breach without undue delay, together with contact details of the Group DPO.
- 8.4 Where a Personal Data Breach occurs, details of the facts relating to the Personal Data Breach, its effects and the remedial action taken will be documented, and such documentation can be made available to the Information Commissioner upon request.
- 8.5 In relation to the processing of Third Party Personal Data, each BT Data Processor and BT Sub-Processor will: (i) implement security and organisational measures that as a minimum meet the requirements of UK laws and also meet any particular measures specified in the relevant Data Processing Agreement; (ii) assist the Third Party Data Controller in ensuring compliance with the obligations set out in Article 25, 32 to 36 and 47.2.d of the UK GDPR, taking into account the nature of the processing and information available to the BT Data Processor or BT Sub-Processor, as applicable; and (iii) in case of a BT Data Processor, inform the Third Party Data Controller, and in case of a BT Sub-Processor, inform the BT Data Processor, of any relevant Third Party Personal Data security breach leading to the accidental or unauthorised loss, alteration, unauthorised disclosure of, or access to, Third Party Personal Data (a "**Third Party Personal Data Breach**") without undue delay after becoming aware of such Third Party Personal Data Breach.
- 8.6 In relation to the processing of BT Personal Data, BT Data Processors will inform the BT Data Controller, and each BT Sub-Processor will inform the BT Data Processor, of any Personal Data Breach relating to BT Personal Data without undue delay after becoming aware of such Personal Data Breach.
- 8.7 The specific security and organisational measures that will be implemented in order to protect Personal Data are set out in Appendix C to these Rules.

9. Internal Processing of Personal Data

- 9.1 Each BT Data Processor will follow the instructions of, and be bound by, the relevant Data Controller entity in relation to the processing of Personal Data.
- 9.2 Each BT Data Processor will be entitled to sub-contract the processing of Personal Data to a BT Sub-Processor, provided that, the Data Controller has provided its prior specific or general authorisation (as, in the case of a Third Party Data Controller, specified in the relevant Data Processing Agreement).
- 9.3 The prior specific or general authorisation of the Third Party Data Controller, as referred to in paragraph 9.2 above, may be provided as a general consent for all sub-processing activities in respect of the relevant Third Party Personal Data, or on a case by case basis. If a general authorisation is provided, then the relevant BT Data Processor will keep the Third Party Data Controller informed of any changes concerning the addition or replacement of BT Sub-Processors as soon as practicable, so that the Third Party Data Controller can object to the change and provided that the objection cannot be remedied, terminate the Third Party Personal Data processing arrangement, subject to the terms and conditions of the relevant Data Processing Agreement, before Third Party Personal Data is passed to the relevant BT Sub-Processor.
- 9.4 Where a BT Data Processor acts for a BT Data Controller and the BT Data Controller is required by UK Data Protection Legislation to put in place safeguards in respect of Personal Data transferred to data processors, the BT Data Processor shall comply with the obligations of a data processor as set out in Article 28(3) of the UK GDPR. In the absence of a specific contract with the BT Data Controller setting out these obligations the BT Data Processor will comply with the General Processor Requirements as set out in Appendix E to these Rules.

10. External Processing of Personal Data

- 10.1 A BT Group Company may only transfer Personal Data to an external processor in accordance with the requirements and instructions of the Group DPO.
- 10.2 Where a BT Data Controller uses an external processor to process Personal Data the BT Data Controller will:
- 10.2.1 make sure that the processor provides sufficient guarantees that their processing will meet the requirements of the UK Data Protection Legislation and ensure the protection of the rights of individuals including that there are appropriate security and operational measures governing the processing of the Personal Data;
 - 10.2.2 make sure that the processor continues to comply with those guarantees; and
 - 10.2.3 enter into a written contract with the processor which will require the processor to only act on the BT Data Controller's instructions and implement and comply with appropriate technical and organisational measures in such a manner that the processing will meet the requirements of UK Data Protection Legislation and ensure the protection of the rights of the Individuals.
- 10.3 Where a BT Data Controller transfers Personal Data to an external third party processor based outside of the UK and not in an Approved Country, in addition to the obligations set out in paragraph 10.2.1 and 10.2.2 above, the BT Data Controller will comply with the rules on the transfer of Personal Data to third countries (as set out in Articles 44 to 50 of the UK GDPR) which may be by entering into the UK Standard Contractual Clauses with the processor in advance of the transfer. When the UK Standard Contractual Clauses are used, this will satisfy the requirement for a written contract as set out in paragraph 10.2.3 above.
- 10.4 Where a BT Data Controller, transfers Personal Data to an external controller based outside of the UK and not in an Approved Country, the BT Group Company will comply with the rules on transfer of Personal Data to third countries (as set out in Articles 44 to 50 of the UK GDPR) by entering into the UK Standard Contractual Clauses with the external controller.
- 10.5 A BT Data Processor will only be entitled to use an external sub-processor to process Third Party Personal Data with the prior specific or general authorization as specified in the relevant Data Processing Agreement with the Third Party Data Controller as set out in paragraph 10.6 and in compliance with the relevant rules on the transfer of Personal Data to third countries (as set out in Articles 45-47 of the UK GDPR). The BT Data Processor will also be required to enter into a written Sub-Processing Agreement with the external sub-processor under which the external sub-processor must agree to:
- 10.5.1 implement and comply with appropriate technical and organisational measures to ensure a level of security appropriate to the risk including protecting the Third Party Personal Data against accidental or unlawful destruction loss, alteration, unauthorised disclosure or access;
 - 10.5.2 only act on the BT Data Processor's instructions that the BT Data Processor itself received from the Third Party Data Controller (unless otherwise required to do so by law) (save to the extent it would put the BT Data Processor in breach of UK Data Protection Legislation, including Articles 45-47 UK GDPR);
 - 10.5.3 comply with such additional requirements of Article 28(4) of the UK GDPR; and
 - 10.5.4 otherwise respect the same data protection obligations applicable to the BT Data Processor in the relevant Data Processing Agreement and paragraphs 1.4, 4.3, 7.5, 8.5, 9.1, 10.5-10.6, 13.7-13.8, 14.2-14.8 and 15 of these Rules.
- 10.6 If a general authorisation is provided, as referred to in paragraph 10.5 above, then the relevant BT Data Processor will keep the Third Party Data Controller informed of any intended changes concerning the addition or replacement of external sub-processors as soon as practicable, so that the Third Party Data Controller can object to the change and provided that the objection cannot be remedied, terminate the Third Party Personal Data processing arrangement, subject to the terms and conditions of the relevant Data Processing Agreement, before Third Party Personal Data is passed to the relevant sub-processor.

11. Assurance and Audit

- 11.1 BT's internal audit function is comprised of three lines of monitoring and audit as follows Together, these functions are implemented in a manner that ensures all aspects and obligations of these Rules are subject to regular verification and compliance checks:
- 11.1.1 **First Line of Monitoring and Audit (Business Frontline):** these are the controls that are in place within each BT Group Company in connection with its day-to-day business such as written policies, operational procedures, risk identification and self-assessment. Controls are designed into systems and processes and operational management is responsible for compliance.
- 11.1.2 **Second Line of Monitoring and Audit (Compliance Function):** these are the functions and executive committees that are in place to provide oversight of the effective operation of the business frontline including defining policies and guidance. Functions include group-wide teams in human resources, finance, security, IT, revenue assurance, legal and regulatory, regulatory compliance and the central Sarbanes-Oxley team. These functions are responsible for reviewing the management of risks at group, line of business and business unit level. Each function reports upon their work undertaken and significant findings to the appropriate executive risk oversight committees including: the executive committee; commercial facing unit audit committees; health and safety, security, global sourcing, ethics, data protection (which includes compliance with these Rules), corporate social responsibility and global sourcing committees; and the group risk panel. These functions may also report to BT Ltd board's audit committee/risk committee as described in relation to the "Third Line of Monitoring and Audit" below. The regulatory compliance function carries out risk based annual reviews of compliance with these Rules and reports its findings to the board appointed executive and oversight sub-committees including: (i) the data governance risks and assurance group, (ii) the business specific audit and risk committee, (iii) the group compliance panel; and (iv) the regional governance committees.
- 11.1.3 **Third Line of Monitoring and Audit (Internal Audit):** this is the independent assurance provided by the BT Ltd board audit and risk committee and the internal audit function that reports to that committee. Internal audit undertakes a programme of regular risk and compliance-based audits covering all aspects of both the first and second lines of monitoring and audit, including in relation to compliance with these Rules and verification that corrective actions identified by audits have been duly implemented. The findings from these audits are reported to the Group DPO, as well as all four lines of monitoring and audit: operational management; the executive and oversight sub-committees including: (i) the data governance risks and assurance group, (ii) the business specific audit and risk committee, (iii) the group compliance panel, (iv) the regional governance committees; and the BT Ltd board audit and risk committee. Such audits are conducted on a cyclical basis, with the frequency for each area determined by a risk-based assessment, but ensuring that all aspects of the Rules are subject to audit over a planned cycle.
- 11.2 Corrective actions are taken by the appropriate persons where a need for this is identified by reviews or audits carried out pursuant to paragraphs 11.1.1 to 11.1.3 above.
- 11.3 Subject to paragraph 11.7 below, summaries of the reviews described in paragraph 11.1.2 in relation to processing activities carried out in respect of Third Party Personal Data by BT Data Processors will be made accessible to the relevant Third Party Data Controller upon its reasonable request, subject to and in accordance with the terms and conditions of the relevant Data Processing Agreement.
- 11.4 Subject to paragraph 11.7 below, where a Third Party Data Controller has received the summaries referred to in paragraph 11.3, and can demonstrate that such summaries are not sufficient for that Third Party Data Controller's legitimate purposes, a BT Data Processor and BT Sub-Processor will accept, at the reasonable request of the relevant Third Party Data Controller, to submit their Personal Data processing facilities for audit of those processing activities relating to the Third Party Personal Data of that Third Party Data Controller. The audit will be: (i) carried out by the Third Party Data Controller or independent and professionally qualified auditors selected by the Third Party Data Controller (where applicable in agreement with the Information Commissioner); (ii) at the Third Party Data Controller's sole expense (such expense to include BT's expenses in responding to and engaging with the audit); (iii) subject to the BT Data Processor and/or BT Sub-Processor's confidentiality requirements; and (iv) carried out without unreasonable disruption to the relevant BT Data Processor and/or BT Sub-Processor.
- 11.5 Subject to paragraph 11.7 below, a BT Group Company will communicate the outcome of any review or audit in its jurisdiction or in relation to Personal Data processed under these Rules that is carried out under paragraphs 11.1.2 or 11.1.3, to the Information Commissioner upon request.

- 11.6 Subject to paragraph 11.7 below, a BT Group Company will allow the Information Commissioner to audit that BT Group Company in order to gather the information necessary to demonstrate the BT Group Company's compliance with these Rules.
- 11.7 BT Group Companies will only share information with, and permit audits by:
- 11.7.1 the Information Commissioner, to the extent strictly required by this paragraph 11 and in accordance with UK laws and provided that: (i) the information and/or audit relates only to compliance with these Rules; and (ii) the information and/or audit is not subject to legal professional privileged (or benefits from similar or related form of legal, professional or litigation privilege anywhere in the world); or
 - 11.7.2 the relevant Third Party Data Controller (in the absence of specific other contractual arrangements with regard to information sharing and audits between the Third Party Data Controller and the relevant BT Group Company), to the extent strictly required by this paragraph 11 and in accordance with Applicable Data Protection Legislation and provided that: (i) the information and/or audit relates only to compliance with these Rules; (ii) the information and/or audit does not contain or involve any commercially sensitive information or draft or preparatory documents relating to or owned by any BT Group Company, or any of their respective clients; (iii) the information and/or audit does not contain or involve any confidential information relating to or owned by a third party; (iv) the information and/or audit is not privileged (or benefits from similar or related protections anywhere in the world); and (v) disclosure of the information or conduct of the audit would not be in conflict with any Applicable Law.
- 11.8 BT Group Companies will immediately notify the relevant Third Party Data Controller if, in that BT Group Company's opinion, an instruction from that Third Party Data Controller in relation to the sharing of information or audit activities in accordance with this paragraph 11 infringes the UK Data Protection Legislation.

Compliance Structure

- 11.9 BT's compliance structure is comprised of a Group DPO appointed in accordance with the criteria set out in Article 37 of the UK GDPR, who is supported by a network of privacy professionals. These privacy professionals are aligned to BT's key business lines and report into the Group DPO. In addition, BT has a number of regional data protection leads, which stakeholders have a local remit but interact with BT's wider privacy network on a global basis across all BT Group Companies. Together, these stakeholders form the "BT Privacy Office".
- 11.10 The Group DPO's role is to advise the BT group board of directors, deal with the Information Commissioner's and other data protection authorities' investigations, report annually on compliance with these Rules and oversee and ensure compliance with these Rules at a global level. The Group DPO operates with independence and has a reporting line to the highest management level within the BT Group.
- 11.11 The BT Privacy Office, including BT's network of privacy professionals and regional data protection leads, with support from relevant BT Personnel is responsible for handling complaints from Individuals in all jurisdictions, reporting major privacy issues to the Group DPO and for ensuring monitoring, training and compliance at a local level, including with these Rules.
- 11.12 In the performance of their duties to monitor compliance with these Rules, the Group DPO and the BT Privacy Office shall have the authority to request that an audit be undertaken of any BT Group Company. Such requests will be directed to the relevant assurance functions, and the Second and Third Lines of Monitoring and Audit (as described in clause 11.1) shall give due consideration to these requests when formulating their risk-based audit plans.

12. Conflicts

- 12.1 In the event that any person within a BT Group Company has reasons to believe that Applicable Laws may prevent any BT Group Company from fulfilling its obligations under these Rules and have a substantial adverse effect on how these Rules work that person is required to promptly notify the Group DPO by using [this form](#) or on the following contact details:

Data Privacy Team, BT
Floor 16

1 Braham Street
London

- 12.2 Any transfers of Personal Data to a law enforcement authority must be based on legal grounds according to Applicable Law. In the case of a conflict of laws, it may be necessary to refer to the applicable international treaties and agreements.
- 12.3 In the event that any Applicable Law imposes a higher level of protection for Personal Data than that described in these Rules, then the relevant Applicable Law will take precedence over these Rules in respect of the point of conflict only.
- 12.4 No BT Group Company will be responsible for any breach of these Rules, if and to the extent that compliance with these Rules is prevented by an Applicable Law.

13. Complaints

- 13.1 If an Individual would like to make a complaint in relation to these Rules, he or she can contact us using the contact details below and providing full details of the issue:

Data Privacy Team, BT
Floor 16
1 Braham Street
London

- 13.2 Or otherwise (for all) per email to: cpo@bt.com. Individuals can complain through the online form which can be found on the BT website in the "Access and updating how we use your information section" of the BT Privacy Policy: [BT | GDPR FORM](#)

Procedure for BT Data Controllers

- 13.3 The relevant contact set out in paragraph 13.1 above will:
- 13.3.1 liaise with all relevant internal departments and external businesses and people to deal with the complaint;
 - 13.3.2 acknowledge receipt of the complaint as soon as reasonably practicable, and no later than 5 Working Days after receiving it;
 - 13.3.3 aim to respond substantively to the complaint without undue delay and in any event within one month of receipt of it, although if the complaint is particularly complex or due to the volume of complaints received by a BT Group Company, the response may be extended by a further two months (or such longer period as is permitted under UK Data Protection Legislation). In such cases the BT Group Company will inform the Individual of, and the reasons for, this extension of its response time;
 - 13.3.4 use reasonable endeavours to acknowledge receipt of the complaint and respond substantively to it promptly for matters which are urgent, provided that the Individual making the complaint has made it clear that the matter is urgent, and
 - 13.3.5 have an appropriate level of independence in the exercise of its functions.
- 13.4 If the complaint is rejected, the Individual will be told of this without undue delay, and in any event within one month.
- 13.5 If the complaint is justified, the Individual will be told of this without undue delay and in any event within 10 Working Days after the decision has been made. The relevant contact set out in paragraph 13.1 above will make sure that any corrective actions are taken to deal with the matters raised in the complaint.
- 13.6 In addition to the internal complaints procedure set out in this paragraph 13, Individuals are entitled to make a complaint directly to the Information Commissioner or to bring a claim for remediation and/or compensation before a competent Court of the United Kingdom.

Procedure for BT Data Processors

- 13.7 Where any BT Data Processor or BT Sub-Processor receives a complaint from an Individual in relation to Third Party Personal Data the BT Data Processor or BT Sub-Processor will forward the complaint or request to the relevant Third Party Data Controller without delay and without obligation to handle it (unless otherwise agreed with the Third Party Data Controller). Although BT encourages Individuals to contact the Third Party Data Controller directly, it still allows them to submit requests and/or complaints including with regards to a breach of UK Data Protection Legislation or these Rules through the procedure outlined in 13.1, 13.2 to 13.5 above.
- 13.8 In the event that the relevant Third Party Data Controller disappears factually, ceases to exist in law or becomes insolvent the complaint or request from the Individual will be dealt with in accordance with the procedure set out in paragraphs 13.1, 13.3 to 13.6 above and BT will, to the best of its ability handle the Individual's complaint.

14. Third Party Beneficiary Rights and Liability

Rights and liabilities applicable to BT Data Controllers

- 14.1 In the event that an Individual suffers material or non-material damage as a direct result of a breach by a BT Data Controller of the provisions contained within Clauses 4 (Privacy Principles), 6 (Transparency and Information Access), 7 (Rights of Individuals), 8 (Security and Confidentiality), 9.4 (Internal Processing of Personal Data), 10.2 (External Processing of Personal Data), 12 (Conflicts), 13 (Complaints), 14 (Third Party Beneficiary Rights and Liability), 15 (Cooperation with the Information Commissioner, Third Party Data Controllers and BT Group Companies) and 18 (Governing Law) of these Rules or the UK Data Protection Legislation then, subject to the limitation of liability provisions set out in paragraph 14.12-14.13 below, the Individual is entitled to (i) lodge a complaint before the Information Commissioner or (ii) bring a claim for remediation of the relevant breach (where the breach is remediable) and/or compensation as a third party beneficiary directly against BT. It is agreed that BT Ltd shall be the legal entity with delegated responsibility for the Rules ("**the Responsible BT Group Company**") and which shall accept liability for the breach as if it had arisen from its own act or omission and must take necessary action to remedy the breach and shall, subject to paragraphs 14.9 to 14.13, compensate the Individual for any damages suffered. While it is not required, Individuals are encouraged first to report their concerns directly to the contacts in paragraph 13 rather than to the Information Commissioner.

Any references to "damages" in this paragraph 14 shall be deemed to include both material and non-material damages.

Rights and Liabilities applicable to BT Data Processors

- 14.2 In the event that an Individual suffers damage as a direct result of a breach by a BT Data Processor, BT Sub-Processor or external sub-processor engaged by it, of its obligations under the UK Data Protection Legislation specifically directed to processors, or of its processor-specific obligations under 4.3, 6.1, 6.2, 7.5, 8.5, 9, 10.5, 10.6, 12, 13.7, 15 of these Rules, then, subject to the limitations set out in paragraphs 14.12-14.13, that Individual is entitled to bring a claim for compensation directly against the Responsible BT Group Company.

Rights enforceable against BT in the absence of the Third Party Data Controller

- 14.3 In addition to the rights set out in paragraph 14.2, if an Individual is unable to bring a claim against the relevant Third Party Data Controller for a breach of these Rules or the UK Data Protection Legislation because the Third Party Data Controller has factually disappeared, ceased to exist in law, or has become insolvent, and no successor entity has assumed the legal obligations of the Third Party Data Controller by contract or by operation of law, then the Individual is entitled to bring such a claim directly against the Responsible BT Group Company as if it were the controller, in respect of the same provisions of these Rules that are enforceable against a BT Data Controller under clause 14.1. In such circumstances, the Responsible BT Group Company shall accept liability for the breach and must take necessary action to remedy it and compensate the Individual for any damages suffered, subject to the limitation of liability provisions in clauses 14.12 to 14.13
- 14.4 The BT Data Processor of Personal Data may not rely on a breach by a relevant BT Sub-Processor or external sub-processor of its obligations in order to avoid its own liabilities.
- 14.5 Where the BT Data Processor and a Third Party Data Controller are involved in the same processing of Personal Data and are both found to be responsible for any damage caused to an Individual by such

processing, the Individual may receive compensation for the entire damage from the Responsible BT Group Company or the Third Party Data Controller.

- 14.6 The relevant jurisdiction for the claim shall be a competent Court of the United Kingdom or, at the Individual's option, the courts of the country where the Individual has their habitual residence and the Individual must agree to submit to the jurisdiction where the claim is made.
- 14.7 These Rules are, where there is a separate agreement, either incorporated by reference (including a link to enable electronic access to these Rules) into the relevant Data Processing Agreement(s) or annexed to the relevant Data Processing Agreement(s), and each Data Controller has the right, subject to paragraphs 14.12 -14.15, to bring a claim for remediation (where remediation is possible) and/or compensation for damage suffered in respect of any breach in relation to Personal Data of:
- 14.7.1 these Rules, against either the BT Group Company that is alleged to have caused the breach, or the Responsible BT Group Company in respect of any breach of these Rules caused directly by a BT Data Processor; or
 - 14.7.2 these Rules (including Appendix E) or the relevant Data Processing Agreement, against the Responsible BT Group Company or the relevant BT Sub-Processor that is alleged to have caused the breach in respect of any breach of these Rules (including Appendix E) or the relevant Data Processing Agreement caused directly by a BT Sub-Processor acting on behalf of that BT Data Processor; or
 - 14.7.3 any relevant Sub-Processing Agreement against the Responsible BT Group Company in respect of a breach of the Sub-Processing Agreement by an external sub-processor appointed under that Sub-Processing Agreement.
- 14.8 Individuals and Third Party Data Controllers may bring claims under these Rules in any competent court, including but not limited to the courts of their country of residence, the country where the breach occurred, or the United Kingdom.

Burden of Proof

- 14.9 Subject to paragraphs 14.12 -14.15 below each BT Group Company acknowledges that: in the event that an Individual or Data Controller can establish facts which show that it is likely that he/she/it has suffered damages as a result of a breach and is entitled to make a claim under this paragraph 14 the burden of proof rests with the Responsible BT Group Company to demonstrate that the BT Group Company or the external sub-processor that is alleged to have caused the breach is not liable for the breach resulting in the damages claimed by the Individual or Data Controller.
- 14.10 In the event that the Responsible BT Group Company can prove that a relevant BT Group Company or external sub-processor is not liable for the alleged breach, then the Responsible BT Group Company and the BT Group Company and/or external sub-processor alleged to have committed the breach may discharge themselves from any responsibility in connection with any claim made by an Individual or Data Controller on the basis of that alleged breach.
- 14.11 If it is held that a BT Group Company or external sub-processor has breached these Rules, a relevant Data Processing Agreement or any relevant Sub-Processing Agreement (as applicable) it will be the responsibility of the person who brought the claim to prove that he or she suffered damage as a result of such a breach and to prove the amount of the damage.

Limitation of liability

- 14.12 To the maximum extent permitted by Applicable Laws, no BT Group Company shall be liable for:
- 14.12.1 any damages which it has proven not to be responsible for in any way;
 - 14.12.2 punitive or exemplary damages (i.e. damages intended to punish a party for its conduct, rather than to compensate the victim of such conduct); or
 - 14.12.3 indirect loss, consequential loss or special damages, howsoever caused. Nothing in this Clause 14.12.3 shall be construed as limiting or excluding any liability for non-material damage suffered by an Individual as a result of a breach of these Rules.

- 14.13 In any event, for the purposes of determining the final amount payable, the Responsible BT Group Company will only be liable for damages which have been:
- 14.13.1 agreed by the Responsible BT Group Company under a signed settlement or compromise agreement with the relevant Individual or Third Party Data Controller making the claim; or
 - 14.13.2 awarded against the Responsible BT Group Company by a judgment that cannot be appealed or under a court order, or by any other legal award made by a court or tribunal with valid jurisdiction.
- For the avoidance of doubt, this clause governs the process for finalising a claim and does not affect the existence of liability, which arises at the time of the breach of these Rules.
- 14.14 In any event and to the maximum extent permitted by Applicable Laws, where the Responsible BT Group Company has paid damages to any Individual under paragraph 14, it shall be entitled to claim back such amount (up to the maximum amount of £3million and to the extent permitted by Applicable Laws) from the applicable BT Data Controller(s), BT Data Processor(s) or BT Sub-Processor(s) responsible for the breach of these Rules or UK Data Protection Legislation.
- 14.15 Notwithstanding any other provision of these Rules and to the maximum extent permitted by Applicable Law, the total liability of BT under these Rules to a Third Party Data Controller shall not exceed the unexhausted cap on liability in the relevant Data Processing Agreement between any BT Group Company and any member of the relevant Third Party Data Controller's group of companies.

15. Cooperation with the Information Commissioner, Third Party Data Controllers and BT Group Companies

- 15.1 All BT Group Companies co-operate and help one another to deal with any:
- 15.1.1 request by an Individual, including for a copy of their Personal Data;
 - 15.1.2 complaint by an Individual, or
 - 15.1.3 inquiry or investigation by the Information Commissioner.
- 15.2 The Information Commissioner has regulatory oversight over all UK BCR Members, including those located outside the UK, to ensure compliance with these Rules. Each BT Group Company will respect and comply with any advice given by the Information Commissioner on any issues regarding the interpretation of these Rules and comply with any formal decisions or notices issued by the Information Commissioner.
- 15.3 Transfer Risk Assessment and Ongoing Monitoring:
- 15.3.1 Before making any transfer of Personal Data under these Rules to a BT Group Company in a third country, the transferring entity must assess whether the laws and practices of the destination country prevent the receiving entity from fulfilling its obligations under these Rules. This assessment must consider:
 - (a) the specific circumstances of the transfer, including purposes, types of entities involved, economic sector, categories and format of personal data, and location of processing;
 - (b) the laws and practices of the third country relevant to the transfer circumstances, including those requiring disclosure to public authorities and applicable limitations and safeguards;
 - (c) any relevant contractual, technical or organisational safeguards put in place to supplement the BCR safeguards.
 - 15.3.2 If any BT Group Company reasonably believes that a BT Data Controller or BT Data Processor is subject to a legal requirement (including any legally binding request for disclosure of the

personal data by a law enforcement authority or state security body) in a country outside the UK that is likely to have a substantial adverse effect on the guarantees provided by these Rules, that BT Group Company shall promptly notify the Group DPO using the details set out at paragraph 12.1 above. If, upon receipt of such notice, the Group DPO agrees that the legal requirement to which the relevant BT Group Company is subject is likely to have a substantial adverse effect on the guarantees provided by these Rules, the Group DPO will notify the Information Commissioner such notice to include information about the data requested, the requesting body, and the legal basis for that disclosure, unless prohibited from doing so by Applicable Law.

- 15.3.3 The Group DPO and the Responsible BT Group Company must be informed and involved in any transfer impact assessment and of any supplementary measures which are put in place.
- 15.3.4 BT Group Companies must monitor on an ongoing basis, and where appropriate in collaboration with data importers, for developments in third countries where Personal Data is processed that could affect the level of protection provided by these Rules.
- 15.3.5 Any BT Group Company acting as data importer must promptly notify the data exporter if it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under these Rules, including following a change in laws or a disclosure request. This information must also be provided to the Responsible BT Group Company.
- 15.3.6 Upon receiving such notification, the Group DPO and Responsible BT Group Company will promptly identify supplementary measures to be adopted. If supplementary measures cannot ensure adequate protection, or if instructed by the Information Commissioner, the relevant transfers must be suspended.
- 15.3.7 If compliance with these Rules cannot be restored within one month of suspension, the transfer must be terminated and any Personal Data already transferred must be returned or destroyed.
- 15.3.8 The Group DPO and Responsible BT Group Company must inform all other BCR members of assessments carried out and results, so that identified supplementary measures are applied to similar transfers or, where effective measures cannot be implemented, such transfers are suspended or terminated.
- 15.3.9 The assessment and any supplementary measures must be appropriately documented and made available on request to the Information Commissioner.

15.4 Public Authority Access Requests:

- 15.4.1 Where any BT Group Company receives or becomes aware of a legally binding request for disclosure of Personal Data by a public authority in a third country, that BT Group Company must:
 - (a) where permitted by applicable law, promptly notify the relevant Data Controller, the Group DPO, and the Responsible BT Group Company, providing all available information including the personal data requested, the requesting authority, legal basis for the request, and response provided;
 - (b) where prohibited from providing notification, use best efforts to obtain a waiver of the prohibition and document those efforts;
 - (c) carefully assess the request for its legality under the laws of the third country and international law, and challenge the request where there are grounds to believe it is unlawful or disproportionate;
 - (d) document its assessment and challenge of the request and, to the extent permitted, make this available to the relevant parties;
 - (e) where disclosure is mandated, interpret the request as narrowly as possible and provide only the minimum amount of information possible based on a reasonable interpretation of the request;

- (f) communicate to the requesting authority that the relevant Data Controller has responsibility for the Personal Data and request that they contact the Data Controller directly; and
- (g) inform the Information Commissioner via the Group DPO of any requests that raise a substantial conflict with the guarantees provided by these Rules.

15.4.2 In the event that a BT Data Processor or BT Sub-Processor has reason to believe that Applicable Law may prevent it from fulfilling the instructions received from the Third Party Data Controller in relation to Third Party Personal Data, or its obligations under these Rules or the relevant Data Processing Agreement, it will promptly notify this to:

- (a) the Third Party Data Controller, which provided that the notification concerns a genuine conflict that cannot be remedied, may be entitled to suspend the relevant data transfer and/or terminate the relevant Data Processing Agreement, subject to the terms of the relevant Data Processing Agreement; and
- (b) the Group DPO; and
- (c) the Information Commissioner,

in each case save to the extent that the relevant BT Data Processor or BT Sub-Processor is prohibited from so notifying.

15.4.3 The BT Data Processor or BT Sub-Processor will communicate any legally binding request for disclosure of Third Party Personal Data by a law enforcement authority to the relevant Third Party Data Controller unless otherwise prohibited, such as due to a prohibition under criminal law in order to preserve the confidentiality of a law enforcement investigation.

15.4.4 On an ongoing basis, the BT Group Company will also:

- (a) provide the data exporter, at regular intervals, with relevant information about requests received, including number, type of data requested, requesting authorities, and outcomes of any challenges;
- (b) preserve information about requests for as long as personal data are subject to BCR safeguards and make available to the Information Commissioner upon request;
- (c) where partially or completely prohibited from providing information to the data exporter, inform the data exporter accordingly without undue delay;

15.4.5 No BT Group Company will transfer Personal Data to any public authority in a third country in a manner that is massive, disproportionate, and indiscriminate and that would go beyond what is necessary and proportionate in a democratic society.

15.5 Cooperation and Information Sharing:

15.5.1 Each BT Data Processor or BT Sub-Processor will: (i) accept that its Third Party Personal Data processing facilities in respect of processing activities carried out on behalf of a Third Party Data Controller, may be audited by the Information Commissioner; and (ii) respect and comply with any advice given by the Information Commissioner on any issues regarding the interpretation of these Rules and comply with any formal decisions or notices issued by the Information Commissioner.

15.5.2 Each BT Data Processor or BT Sub-Processor will, in respect of Third Party Personal Data cooperate and assist the relevant Third Party Data Controller to comply with applicable Data Protection Legislation to the extent reasonably possible and within a reasonable timeframe.

15.5.3 BT Ltd agrees and undertakes that it shall deal promptly and properly with all reasonable requests from any other BT Group Company to procure that another BT Group Company performs its obligations under these Rules and, where required, shall procure such performance by that BT Group Company. Each other BT Group Company shall do all things necessary to assist BT Ltd to enable it to discharge its obligations under this paragraph 15.5.3 and shall provide such cooperation, assistance and information as may be needed by BT Ltd in connection with any claims made by Individuals or Third Party Data Controllers against BT Ltd acting in its capacity as the Responsible BT Group Company under these Rules.

16. New BT Group Signatories and Termination

- 16.1 Subject to the prior agreement of the Group DPO (which will only be provided where the Group DPO is satisfied that the new party is capable of complying with the terms of these Rules), a new party may be added to these Rules provided that it is a member of BT and signs an Agreement of Adherence with BT Ltd to be bound by these Rules. No transfers of Personal Data will be made to a new party until that party is effectively bound by these Rules;
- 16.2 The other parties to these Rules hereby authorise BT Ltd to do this at its reasonable discretion and agree to extend the commitments which they give in this Agreement to the new party, in respect of any Personal Data which they transfer to or receive from the new party.
- 16.3 In the event that the BT Data Controller or BT Data Processor acting as Data Importer ceases to be a BT Group Company, the Data Importer shall securely destroy or return personal data received under the Rules to the Data Exporter and delete existing copies (unless Applicable Law requires storage of the Personal Data, in which case the Data Importer will inform the Data Exporter thereof), unless otherwise instructed by the Data Exporter.

17. Variations to these Rules

- 17.1 From time to time, it may be necessary to change these Rules or add to them. In particular, this may be because of a change:
 - 17.1.1 In UK Data Protection Legislation; or
 - 17.1.2 to the structure of BT's group of companies.
- 17.2 Subject to paragraphs 17.3-17.6, BT Ltd shall be entitled to amend or vary these Rules without the consent of any other BT Group Companies, Individuals or third party, to the extent such amendment or variation is not prohibited by the terms of these Rules, and that this will not reduce the protection afforded to data subjects. BT Ltd shall notify such amendments to the BT Group Companies and such amendments shall come into force 30 days after the date of such notice.
- 17.3 If the Rules are changed or added to in accordance with paragraph 17.2, the Group DPO will:
 - 17.3.1 ensure an up to date version of these Rules is published and publicly available on BT's website (in accordance with paragraph 6.1);
 - 17.3.2 upon request, provide any necessary information to Individuals or the Information Commissioner, or relevant Third Party Data Controllers in respect of such changes and a list of the BT Sub-Processors or external sub-processors referred to in Paragraphs 9.3 and 10.6; and
 - 17.3.3 in the case of substantive changes or additions affecting processing activities carried out by BT Group Companies on behalf of Third Party Data Controllers, report such changes or additions to the relevant Third Party Data Controller.
- 17.4 Without prejudice to paragraph 17.3, BT will notify the Information Commissioner of any changes or additions made during a calendar year to (i) these Rules or (ii) the BT Group Companies which are bound by these Rules, in both cases reasonably promptly after the end of that calendar year, and shall provide a brief explanation of the reasons justifying such changes or additions.
- 17.5 If a change to the Rules would possibly affect the level of protection offered by the Rules or significantly affect their bindingness, impact overall compliance with UK Data Protection Legislation, or be otherwise detrimental to the rights of data subjects, such change must be promptly communicated to the Information Commissioner.
- 17.6 Some changes or additions (particularly those which significantly affect data protection compliance) may need to be authorised by Information Commissioner.
- 17.7 Where paragraph 17.3.3 applies and the change or addition will have a material impact on the conditions under which Third Party Personal Data is processed for the Third Party Data Controller, for example a

change in Sub-Processors or external sub-processors, BT will notify the relevant Third Party Data Controller(s) as soon as practicable in order to enable the Third Party Data Controller(s) to object to the change or addition and provided that the objection cannot be remedied, the Third Party Data Controller(s) may be entitled to change or terminate the relevant Data Processing Agreement, subject to the terms and conditions of the relevant Data Processing Agreement, in advance of implementation of the proposed change or addition.

- 17.8
- Appendix F of these Rules contains a revision history that sets out information about changes made to these Rules, including the date of the change and a summary of the change, which Appendix shall be maintained by the Group DPO.

18.

Governing Law

- 18.1
- These Rules and any dispute or claim arising out of or in connection with it will be governed by and construed in accordance with the law of England and Wales.
- 18.2
- Subject to clause 14 (Third Party Beneficiary Rights and Liability),the courts of England and Wales will have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with these Rules.

This agreement takes effect on the date stated at the beginning of it.

Signed by [insert name of BT Group Company] acting by [insert name of first director] , a director	 [signature] Director
--	--

Appendix A Participating BT Group Companies

Region	Country	Legal Entity Name	Registered Office Address
UK	UK	BPSLP Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	British Telecommunications Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT Global Services Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT Group plc	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT Lancashire Services Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT OnePhone Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT Solutions Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	BT UAE Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	Communications Global Network Services Limited - UK Branch	1 Braham Street, London, E1 8EE, United Kingdom
	UK	Digital Mobile Spectrum Limited	24/25 The Shard, 32 London Bridge Street, London, SE1 9SG, United Kingdom
	UK	Global Security Europe Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	Mainline Digital Communications Limited	Trident Place, Mosquito Way, Hatfield, Hertfordshire, AL10 9BW, United Kingdom
	UK	Numberrapid Limited	1 Braham Street, London, E1 8EE, United Kingdom
	UK	Pelipod Ltd	1 Braham Street, London, E1 8EE, United Kingdom
Europe	Austria	BT Austria GmbH	c/o BDO Assurance GmbH, Wirtschaftsprüfungs- und steuerberatungsgesellschaft Am Belvedere 4, 1100 Wien
	Belgium	BT Global Services Belgium BV	Telecomlaan 9, 1831 Diegem, Belgium
	Belgium	IP Trade SA	129 Rue des Guillemins, Block B, LIEGE, 4000, Belgium
	Czech Republic	BT Global Europe B.V., odštěpný závod	Pujmanové 1753 / 10a, Nusle, 140 00, Prague, 4, Czech Republic
	Denmark	BT Denmark ApS	Havneholmen 29, 1561, Kobenhavn V, Copenhagen, Denmark
	Finland	BT Nordics Finland Oy	Mannerheimvägen 12 B 6, 00100 Helsinki, Finland
	France	BT France S.A.S.	Tour Ariane, 5 place de la Pyramide, La Defense Cedex, 92088, Paris, France
	Germany	BT (Germany) GmbH & Co. oHG	Marcel-Breuer-Straße 6 80807 München
	Germany	Global Security Europe Limited - Germany Branch	Widdersdorfer Strasse 252, 50933, Cologne, Germany
	Hungary	BT ROC Kft	Boldizsár U. 4., Budapest, 1112, Hungary
	Hungary	BT Global Europe B.V. Magyarországi Fioktelepe	Boldizsár u. 4., Budapest, 1112, Hungary

	Ireland	BT Business Telecoms Ireland Limited	2 Grand Canal Plaza, Upper Grand Canal Street, Dublin, 4, Republic of Ireland
	Ireland	The Faraday Procurement Company Limited	5th Floor, 2 Grand Canal Plaza, Upper Grand Canal Street, Dublin 4, Ireland
	Isle of Man	Communicator Insurance Company Limited	Third Floor, St Georges Court, Upper Church Street, Douglas, IM1 1EE, Isle of Man
	Italy	BT Italia S.p.A.	Via Filippo Sassetti 32, 20124, Milano, Italy
	Luxembourg	BT Global Services Luxembourg SARL	12 rue Eugene Ruppert, L 2453 , Luxembourg
	Netherlands	BT Nederland N.V.	Minerva & Mercurius building, Herikerbergweg 2, 1101 CM , Amsterdam Zuidooost, Netherlands
	Norway	BT Solutions Norway AS	Munkedamsveien 45, Oslo, 0121, Norway
	Poland	BT Poland Spółka Z Ograniczoną Odpowiedzialnością	Marszałkowska Centre Ul. Marszałkowska 126/134 00-008 Warsaw, Poland
	Portugal	BT Portugal - Telecomunicações, Unipessoal Lda	Rua D. Francisco Manuel de Melo 21-1, 1070-085 Lisboa, Portugal
	Spain	BT Global ICT Business Spain SLU	C/ María Tubau, 3, 28050 de Madrid, Spain
	Sweden	BT Nordics Sweden AB	Box 30005, 104 25, Stockholm, Sweden
	Switzerland	BT Switzerland AG	Richtistrasse 5, 8304, Wallisellen, Switzerland
India	India	BT e-Serv (India) Private Limited	11th Floor, Eros Corporate Tower, Opp. International Trade Tower, Nehru Place, New Delhi, 110019, India
	India	BT Global Business Services Private Limited	11th Floor, Eros Corporate Tower, Opp. International Trade Tower, Nehru Place, New Delhi, 110019, India
	India	BT Global Communications India Private Limited	11th Floor, Eros Corporate Tower, Opp. International Trade Tower, Nehru Place, New Delhi, 110019, India
	India	BT (India) Private Limited	11th Floor, Eros Corporate Tower, Opp. International Trade Tower, Nehru Place, New Delhi, 110019, India
	India	Tech Mahindra Limited	Gateway Building, Apollo Bunder, Mumbai 400001, Maharashtra, India
US & Canada	Canada	BT Canada Inc.	Regus Brookfield Place, 161 Bay Street, 27th Floor, Toronto ON M5J 2S1, Canada
	USA	BT Americas Inc.	c/o Corporation Service Company, 251 Little Falls Drive, Wilmington DE 19808, United States
	USA	BT Procure L.L.C.	c/o Corporation Service Company, 251 Little Falls Drive, Wilmington DE 119808, United States
	USA	SAFE Securities Inc	3000 El Camino Real, Building 4, Suite 200, Palo Alto CA-94306, United States
LATAM	Argentina	BT Argentina S.R.L.	Maipu No 1210, piso 8 (C1006), Buenos Aires, Argentina
	Brazil	BT Communications do Brasil Limitada	Avenida Doutora Ruth Cardoso , 4777 - 14 andar A, Pinheiros, São Paulo, SP 05477-000, Brazil
	Chile	Servicios de Telecomunicaciones BT Global Networks Chile Limitada	Rosario Norte 407, Piso 6, Las Condes, Santiago, Chile
	Colombia	BT Colombia Limitada	Calle 113, 7-21 Piso 10, Torre A Oficina 1015, Teleport Business Park, Bogota, Colombia
	Costa Rica	BT Global Costa Rica SRL	PROVINCIA 01 SAN JOSE, CANTON 02 ESCAZU, SAN RAFAEL, CENTRO , Edificio A, Cuarto Piso, Oficinas Deloitte, Costa Rica

	Ecuador	BT Solutions Limited (Sucursal Ecuador)	Av. Amazonas N21-252 y Carrión, Edificio Londres, 4° Piso, Quito, Ecuador
	El Salvador	BT El Salvador, Limitada de Capital Variable	Edificio Avante Penthouse Oficina, 10-01 Y 10-03, Urbanizacion, Madre Selva, Antiguo Cuscatlan, La Libertad, El Salvador
	Guatemala	BT Guatemala S.A.	5ta avenida 5-55 zona 14, Edificio Europlaza World Business Center, Torre IV, nivel 7, oficina 702, Guatemala City, Guatemala
	Honduras	BT Sociedad De Responsabilidad Limitada	Boulevard San Juan Bosco, Plaza Ficohsa, 3er nivel, Frente A Ruby Tuesday, Lomas del Gujarro Sur, Tegucigalpa, Honduras
	Jamaica	BT Jamaica Limited	Suite #6, 9A Garelli Avenue, Half way tree, St. Andrew, Kingston 10, Jamaica
	Mexico	BT LatAm México, S.A. de C.V.	Boulevard Manuel Avila Camacho 32. Piso 6. , Colonia Lomas de Chapultepec III Seccion, Miguel Hidalgo, Mexico City , 11000
	Venezuela	BT LatAm Venezuela, S.A.	Calle Guaicaipuro, Urbanizacion El Rosal, Municipio Chacao, Oficina 11B, Piso 11, Torre Forum, Caracas, Venezuela
	Nicaragua	BT Nicaragua S.A.	De donde fué el Restaurante Marea Alta (Ahorra quesillos , El Pipe, 2 cuadras al este, 10 Metros al norte, frente al, Hotel El Gran Marquez, Casa #351, Nicaragua, 2815, Nicaragua
	Paraguay	BT Paraguay S.R.L.	Av. Brasilia N° 767 casi Siria, Asunción, Paraguay
	Peru	BT Peru S.R.L.	AV. Santa Cruz 830, Oficina 301, Miraflores, Lima, Peru
	Puerto Rico	BT Communications Sales, LLC Puerto Rico branch	The Prentice-Hall Corporation System, Puerto Rico, Inc., c/o Fast Solutions, LLC, Citi Tower, 252 Ponce de Leon Avenue, Floor 20, San Juan, Puerto Rico, 00918, Puerto Rico
	Trinidad and Tobago	BT Solutions Limited	2nd Floor CIC Building, 122-124 Frederick Street, Port of Spain, Trinidad and Tobago
	Uruguay	BT Solutions Limited Sucursal Uruguay	Rincón 487 Piso 11, Montevideo, ZIP CODE 11.000, Uruguay
AMEA	Algeria	BT Algeria Communications SARL	20 Micro zone d'Activités Dar El Madina, Bloc B, Loc N01 Hydra, Alger, 16000, Algeria
	Australia	BT Australasia Pty Limited	Level 20, 420 George Street, Sydney, NSW 2000, Australia
	China	BT China Limited	Room 702A, Tower W3, Oriental Plaza, 1 East Chang An Avenue, Dongcheng, Beijing, 100738, China
	China	BT China Communications Limited	Unit 1537B, Floor 15th, No. 55, Xili Road, Shanghai Free Trade Zone, Shanghai, China
	Egypt	BT Telecom Egypt LLC	95 C st. El Sayed El Mirghany, Heliopolis Cairo, Egypt
	Ghana	BT Ghana Limited	5th Floor, Vivo Place, Cantonments City, Rangoon Lane, P.O. Box MB 595, Accra, Ghana
	Hong Kong	BT Hong Kong Limited	38th Floor Dorset House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong
	Hong Kong	Infonet China Limited	38 Floor Dorset House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong
	Indonesia	PT BT Communications Indonesia	20/F of IWG Spaces at World Trade Centre 3, , Jl. Jend. Sudirman, RT.4/RW.2., Karet Kuningan, Kota Administrasi Jakarta Selatan,, Jakarta, 12920, Indonesia
	Israel	B.T. Communication Israel Ltd	Beit Oz, 14 Abba Hillel Silver Rd, Ramat Gan, 52506, Israel

Japan	BT Japan Corporation	ARK Mori Building, 12-32 Akasaka, 1-Chome, Minato-Ku, Tokyo, 107 - 6024, Japan
Kenya	BT Communications Kenya Limited	Aln House, Eldama Ravine close, off Eldama Ravine Road, Westlands, P O Box 764, Sarit Centre, Nairobi, 00606, Kenya
Korea	BT Global Services Korea Limited.	8th Floor, KTB Building, 66 Yeoui-daero, Yeongdeungpo-gu, Seoul, 07325, Korea, Republic of
Lebanon	BT Lebanon S.A.L.	Abou Hamad, Merheb, Nohra & Chedid Law Firm, Chbaro Street, 22nd Achrafieh Warde Building, 1st Floor, Beirut, P.O.BOX 165126, Lebanon
Malawi	BT Malawi Limited	KEZA Office Park Blocks 3, First Floor, Near Chichiri, Shopping Mall, Blantyre, Malawi
Malaysia	BT Global Technology (M) Sdn. Bhd.	Level 5, Tower 3, Avenue 7, Bangsar South, No.8, Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia
Malaysia	BT Systems (Malaysia) Sdn Bhd	Level 5, Tower 3, Avenue 7, Bangsar South, No.8, Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia
Morocco	BT Solutions Limited - Morocco Branch	Bd. Abdelmoumen, Immeuble Atrium, n 374, Lot. Manazyl Al Maymoune, 5eme etage, Casablanca, 20390, Morocco
Nigeria	BT (Nigeria) Limited	Civic Towers, Plot GAI, Ozumba Mbadiwe Avenue, Victoria island, Lagos, Nigeria
Oman	BT International Holdings Limited & Co. LLC	Maktabi Building, Building No. 458, Unit No. 413 (4th Floor, Road No - R4I, Block No. 203, Plot No. 107, Zone No. SW4I, Complex No. 271, Al Watiyah, Bausher, Muscat, Sultanate of Oman, Oman
Pakistan	BT Pakistan (Private) Limited	Cavish Court, A-35, Block 7&8, KCHSU, Shahrah-e-Faisal, Karachi, 75350, Pakistan
Philippines	BT Communications Philippines Incorporated	40th Floor, PBCom Tower 6795, Ayala Avenue cor. Rufino St, Makati City, 1226, Philippines
Qatar	BT Global Services (North Gulf) LLC	1413, 14th Floor, Al Fardan Office Tower, Doha, 31316, Qatar
Russian Federation	BT Solutions Limited Liability Company	Room 62, prem. XX, floor 2, Pravdy, 26, 125124, Moscow, Russian Federation
Singapore	BT Global Solutions Pte. Ltd.	Level 3, #03-01/02 & #03-04, Block B, Alexandra Technopark, 438B Alexandra Road, Singapore, 119968
Singapore	BT Singapore Pte. Ltd.	Level 3, #03-01/02 & #03-04, Block B, Alexandra Technopark, 438B Alexandra Road, Singapore, 119968
Singapore	BT (India) Private Limited Singapore Branch	Level 3, #03-01/02 & #03-04, Block B, Alexandra Technopark, 438B Alexandra Road, 119968, Singapore
South Africa	BT Communications Services South Africa (Pty) Limited	BT Building, Woodmead North Office Park, 54 Maxwell drive, Woodmead, Johannesburg, 2191, South Africa, South Africa
Taiwan	BT Limited Taiwan Branch	Shin Kong Manhattan Building, 14F, No. 8, Sec. 5, Xinyi Road, Taipei, 11049, Taiwan
Tanzania	BT Solutions Limited - Tanzania Branch	Region Dar Es Salaam, District Kinondoni, Ward Msasani, Street Msasani Peninsula, Road I Bains Singh Avenue, , Plot number 1403/I, Ground Floor, 14111, Tanzania, United Republic of
Thailand	BT Siam Limited	No.63 Athenee Tower, 23rd Floor (CEO Suite, Room No.38), Wireless Road, Kwaeng Lumpini, Khet Pathumwan, Bangkok, 10330, Thailand

Tunisia	BT Tunisia S.A.R.L	Rue de l', Euro Immeuble Slim, Block A-2nd floor-Les berges du Lac, Tunis, 1053, Tunisia
Turkey	BT Bilisim Hizmetleri Anonim Şirketi	Acibadem Mahallesi Çeçen Sk. Akasya A , Kule Kent Etabı Apt. No: 25 A/28- , Üsküdar, Istanbul, Turkey
Turkey	BT Telekom Hizmetleri Anonim Şirketi	Acibadem Mahallesi Çeçen Sk. Akasya A , Kule Kent Etabı Apt. No: 25 A/28- , Üsküdar, Istanbul, Turkey
Ukraine	BT Ukraine Limited Liability Company	Office 702, 34 Lesi Ukrainky Boulevard, Kyiv, 01042, Ukraine
United Arab Emirates	BT MEA FZ-LLC	Office No G03, , Ground Floor, EIB Building No 04, Dubai, United Arab Emirates
United Arab Emirates	BT UAE Limited - Dubai Branch (1)	Office no.206 BLOCK B, Diamond Business Center I, Al Barsha South Third, Dubai, P.O.BOX 25205, United Arab Emirates
United Arab Emirates	BT UAE Limited - Dubai Branch (2)	Office no.206 BLOCK B, Diamond Business Center I, Al Barsha South Third, Dubai, P.O.BOX 25205, United Arab Emirates
Vietnam	BT (Vietnam) Co. Ltd.	16th Floor Saigon Tower, 29 Le Duan Road, District 1, Ho Chi Minh City, 710000, Socialist Republic of Vietnam

Appendix B Purposes of Processing

This Appendix refers to the processing that BT undertakes as both a BT Data Controller and as a BT Data Processor.

All of the data processing set out in this Appendix is conducted as a BT Data Controller or a BT Data Processor (on behalf of a BT Data Controller). Where required by a Third Party Data Controller some of these activities marked by an asterisk (or others specified in a Data Processing Agreement) may be carried out as BT Data Processor (on behalf of the Third Party Data Controller).

Typically, BT act as a BT **Data Controller** in respect of the following types of BT Personal Data:

- HR data (including recruitment data) in relation to its Staff.
- Customer data in respect of the services it provides via its BT consumer line of business.
- Customer data in respect of the services it provides to sole traders and limited partnerships via its BT Business line of business.
- Customer's staff data in respect of providing the service.
- Shareholder data in respect of its Shareholders
- Data relating to BT's suppliers or service partners.

HR data is typically only transferred to BT Group Companies acting as a BT Data Controller in non-adequate third countries where a line manager is located in those countries (for general recruitment, HR and financial management purposes) or in respect of access to corporate employee directory type information. Business contact data is typically only transferred to BT Group Companies acting as BT Data Controller in non-adequate third countries for marketing activities, business forecasting and reporting, managing client relationships and ensuring the security of BT's products and services and participation in events.

Where a BT Group Company receives BT Personal Data from another BT Group Company, it may receive that BT Personal Data as a BT Data Controller or a BT Data Processor (or both depending on the nature of the BT Personal Data and the purposes of processing). There are a number of key BT Group Companies in non-adequate third countries which will typically act as BT Data Processors on behalf of BT where common IT systems are used across the Group and where administrative and support functions have been centralised, including India.

There are a number of key BT Group Companies in non-adequate third countries which will typically act as BT Data Processors on behalf of BT where common IT systems are used across the Group and where administrative and support functions have been centralized. These BT Group Companies are generally those located in India, Philippines and Malaysia.

Typically, BT acts as a **Data Processor (on behalf of a Third Party Data Controller)** in respect of:

- Business customer data that it processes in connection with the services it provides to Third Party Data Controllers via its BT Wholesale, Openreach, BT Business and BT Global Services lines of business.

The following definition is used in this Appendix B:

"Associated Person" means, in respect of the relevant Individuals, family members or beneficiaries under insurance policies or other company-provided benefits held for or on behalf of the Individual or their family members or beneficiaries.

"contractor" means a third party working for a relevant entity who is not an employee of that relevant entity.

"employee" means individuals employed by the relevant entity.

"staff" means employees and contractors.

The below table provides a high-level overview of routine transfers between the BT Group Companies

Activity Group / Category	Activities	EEA > UK	EEA > India	EEA > US	EEA > Third Countries (All Others)
B2B Customers	- Contact details for staff of corporate customers - Data about end-users of BT B2B managed services (e.g. IP addresses, call data records)	✓	✓	✓	✓
HR	- Absence administration - Bill, Invoice and payments - Diversity & Inclusion - Employee exit - Employee relations and managing employee performance - Employment tax - Health & Safety - Learning, training and development - Recruitment - Rewards, benefits and compensation (including connected and related persons (such as children of employees)) - Workforce administration and management	✓	X	X	X
HR	New Colleague Onboarding	✓	✓	X	X
HR	BT Staff data re performance if Staff manager is abroad	✓	✓	✓	✓
Facility & Property	- CCTV - Managing building access & security - Facility operations - Logistics and transportation - Manage real estate and commercials	✓	X	X	X
Finance	Financial planning, reporting and account management	✓	✓	X	X

Activity Group / Category	Activities	EEA > UK	EEA > India	EEA > US	EEA > Third Countries (All Others)
	Process accounts receivable, payable and expense reimbursements				
Finance	Financial Accounting and Reporting	✓	✓	X	X
IT	IT incident management	✓	X	X	X
Legal	- DSARs - Law enforcement Disclosures - Managing regulator relationships - Perform assurance/audits - Risk governance	✓	✓	X	X
Procurement	- Service Assurance - Acquiring goods & services	✓	✓	X	X
Procurement	Sourcing and contracting	✓	✓	X	X

Please note, in relation to Openreach Commercial Information or Confidential Customer Information, BT must follow strict guidelines set out in our Information Sharing Agreements.

This table primarily describes the purposes of processing of BT Personal Data by BT Group Companies acting as BT Data Controllers located in the UK. A high-level explanation of what BT Personal Data is actually transferred to other BT Group Companies and why is outlined above.

Data Subjects	Data Types	Purposes of Processing
Individuals whose data may be processed by a BT Group Company in connection with BT's business activities including: • Consumer and business customers, sole traders and unlimited partnerships; • Employees, contractors, users and customers of BT's corporate and business customers, suppliers, partners, agents, and subscribers; and • their Associated Persons.	• Contact details such as name, address, contact number, including mobile and email address. • Payment information, such as direct debit or credit card details. • Information about spouses and/or financial associates. • Phone records including numbers dialled, the time and the length of calls and call recordings. • Information about goods or services provided. • Usage data about how our services are used, such as customer devices and viewing cards, channels and programmes watched and adverts and services accessed, and IP addresses and other traffic data including websites visited, records of whether or not parental controls have been activated and the level of activation selected, and high-level user behaviour. • Special categories of personal data in relation to physical or mental health details, racial or ethnic origin and religious or other beliefs. • Images including photographs, videos and CCTV images.	• To provide to individuals and companies services such as, among others, information technology, electronic communication and security services including telephone, mobile, TV, and internet services. • To charge for services and let customers know if we make changes to services. • To validate identity of individuals if they get in touch with us, to help protect our customers from identity theft and fraud, and to prevent and detect crime or money laundering. • To perform credit checks. • If the customer agrees, to publish their details in the Phone Book and other directories. • Unless the customer tells us otherwise, to make contact from time to time, to tell the customer about products or services we think they might be interested in. • To provide personalised services such as viewing recommendations and tailored advertising. • If we think there's been crime, fraud, misuse of, or damage to, our network, we'll use information for our internal investigations and any subsequent prosecution(s). • Where required by law, we retain and disclose information about how customers use our services, for example for crime prevention and to protect national security. • Monitoring communications with us for training purposes, quality assurance, to record details about the products and services customers order from us, and in order to meet our legal and regulatory obligations generally. • To help us understand and manage traffic flows on our network. This includes IP addresses and other traffic data including websites visited. We may also use this information to provide customers with certain services that they have asked us for, like parental controls on web access. • If we think there's been crime, fraud, misuse of, or damage to, our network, we'll use customer information for our internal investigations and any subsequent prosecution(s). We will also provide it in reply to other lawful requests for information such as about illegal online file sharing. • To check if customers want to activate parental controls or not. • To authenticate customers' identities when they sign in. • To keep improving the way our website works. • We use website usage data in bulk and anonymously to give us insights into new products and services our customers might like. • Performing behavioural analysis. • Debt collection.

- Providing consultancy and advisory services to customers.
- Undertaking surveys and research.
- Advertising BT's businesses, activities, goods or services and promoting public relations in connection with those businesses, activities, goods or services.
- Keeping accounts related to any business or other activity carried on by BT, or deciding whether to accept any person as a customer or supplier, or keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by him or to him in respect of those transactions, or for the purpose of making financial or management forecasts to assist him in the conduct of such business or activity.
- In order to analyse communications spend and structure and to highlight to our clients' areas of waste, inefficiency and cost savings.
- Assisting our customers with support and maintenance activities in relation to our products and services.
- In order to provide real-time/historic recording, reporting, contact prioritisation and management tools to our customers.
- Providing customers with accurate usage data and in order to assist customers with improving financial forecasting and budgeting.
- In order to provide effective security and risk management products to our customers including monitoring our customers traffic profiles.
- To provide our customers with fully managed and automated ID services.
- To provide technical support of products and services.

Shareholders	• Contact details, such as name, address, contact number, including mobile and email address. • Account information • Tax information • Transaction information	• Administration of shares and payments of dividends. • Compliance with legal and regulatory obligations.
Staff (including applicants, candidates, existing and former staff, contractors and pension members) and persons nominated by candidates or staff (including connected and related persons (such as children of employees), emergency contacts, references contacts and brokers)	• Name • Gender and Title • Addresses • Country of Residence • Telephone and Fax Numbers • Email Addresses • Identification Data • Date and Place of Birth • Nationality • Family • Marital Status • Curriculum Vitae Information (e.g. hobbies/interests, references) • Employment Details • Connected and Related Persons	• Recruitment and Job Applications • Screening • HR Administration and Management • Global Directories • Planning and Work Organisation • Absence, Sickness and Maternity Administration • Mobility (e.g. travel, secondments, transfers, relocation) • Remuneration and Payroll • Benefits and Reward Administration (e.g. car scheme administration and share scheme administration) • Pension Administration and Fund Management • Performance Assessment and Management • Learning, Training, Knowledge Sharing and Development • Workplace and Event Management • Company Asset Management and Protection

- Pension Details
- Financial Data
- Insurance Details
- Social Security Number
- Tax Information
- Sales Data
- Correspondence (e.g. email)
- Complaint Information
- Transaction Information
- IP address
- Location Data
- Electronic Traffic Data
- Images
- Voice and video recordings
- Gifts and Entertainment Details
- Background Information/Screening Data
- Dietary/Special Requirements
- Medical Data/Sickness/Disability
- Race/Ethnicity
- Religion/Beliefs
- Sexual Orientation
- Union Membership
- Biometric Data

- Expenses Management
- Travel Management
- HR Dispute Management (including disciplinary, capability and grievance)
- Transaction Management
- Monitoring
- Whistleblowing (hotline support and investigation)
- Marketing
- Measuring and advancing diversity and inclusion within the organisation
- Provision of workplace tools and systems
- Employee surveys

Data Subjects*

- All Data Types

- Network management
- Information Technology (IT) Management (including planning, organising, acquiring, developing, implementing, delivering, maintaining and servicing, supporting, monitoring, evaluating and testing the IT infrastructure (solutions, systems (e.g. email systems), software, hardware, databases, applications, websites, cookies profiling, platforms and other IT related functions), the users of the IT infrastructure and the data held on the IT infrastructure)
- Information Management and Data Storage (including back-ups)
- Business Continuity Management
- Security Management (including company and personnel security and access control administration and management)
- Identification and Verification
- Screening
- Crime and Fraud Prevention, Monitoring, Detection and Management (including Financial Crime, Anti-Money Laundering, Sanctions, Bribery and Corruption)
- Audit, Monitoring, Conformance Checks and Testing
- Compliance with Legal and Regulatory Requirements (including conflicts of interests and risk review and analysis)
- Quality Control and Process Monitoring

- Management Information and Reporting
- Complaint/Query Management
- Statistical Reports and Analytics
- Project Management
- Facilities Management
- Mergers and acquisitions

Appendix C Security and Organisational Measures

1. Introduction

This Appendix sets out the security and organisational measures implemented by BT Group Companies to protect Personal Data processed under these Rules. These measures ensure appropriate technical and organisational security in accordance with Data Protection Legislation requirements and are applied using a risk management approach across all BT products and services. BT places security at the centre of the business, pulling together cyber, physical and personnel security teams into one function. Driving increased security automation and ensuring our new platforms are designed with enhanced Security at their core.

2. BT Security Policy

BT's Security Policy protects BT Group Companies, customers, and partners from cyber threats through a comprehensive framework covering people, premises, information, and assets throughout the information lifecycle. The policy is built upon nine key principles:

- business practices alignment with laws and regulations
- data quality assurance
- evaluation mechanisms for compliance validation
- compliance activities including checks and monitoring
- risk-based evidenced decisions
- company values and reputation maintenance
- breach investigation and remediation
- appropriate disciplinary action
- continuous improvement of the Information Security Management System to address evolving threats and regulatory requirements

The policy mandates eighteen key security control domains including:

- Inventory and control of enterprise assets
- Inventory and control of software assets
- Data protection throughout the lifecycle
- Secure configuration
- Account management
- Access control management
- Continuous vulnerability management
- Audit log management
- Email and web browser protection
- Malware defences
- Data recovery
- Network infrastructure management
- Network defence and monitoring
- Security awareness training
- Service provider management
- Application software security
- Incident response management
- Penetration testing

3. BT Security Standards

BT Group Security Standards set out the expected minimum level of security requirements along with agreed repeatable, verifiable way of doing things to protect BT Group assets inclusive of BT Group Technology Systems, BT Networks, BT Group Information and client Information. Under our Security Policy we have 22 mandatory security standards:

Category	Standard	Description
Governance and Management	Security Governance	Aims to establish, maintain, and monitor an information security governance framework that enables the governing body to set clear direction for and demonstrate commitment to information security and risk management.
	Security Management	Establishes a comprehensive framework for managing information security within BT, covering policy development, compliance, security organisation, project management, and local environment security to ensure effective and consistent application of security practices throughout BT.
	People Management	Embeds information security requirements into every stage of the employment lifecycle, establish security agreements with individuals or external parties accessing critical or sensitive information and systems, and assign ownership of critical business environments, processes, applications, and information to capable individuals.
	Security Assurance	Implements a consistent and structured information security assurance program, supported by comprehensive security testing, security measurement, and regular security and risk monitoring.
	Acceptable Use	Outlines the acceptable use of IT equipment and assets emphasising the importance of securing information and assets to prevent security incidents.
Technical Infrastructure and Systems	Hardware and Endpoint Devices	Manages the lifecycle of all types of hardware securely, including endpoint devices, office equipment, and specialist devices, addressing information security requirements for their acquisition, configuration, maintenance, and disposal.
	Technical Infrastructure	Design and build secure system and network installations to operate efficiently, protect against cyber threats, and support current and future workloads.
	User Applications	Implements procedural and technical security controls to protect email systems and collaboration platforms, ensuring their availability, maintaining the confidentiality and integrity of messages and information in transit, and minimizing the risk of misuse or unauthorised disclosure.
	Industrial Control Systems	Establish a governance program over industrial control systems (ICS) to manage security elements in a structured, consistent, and effective manner, subjecting critical ICS to specialised risk assessments and tailored security controls.
	System Resilience	Implement a system resilience programme to ensure robust, reliable infrastructure, manage capacity, apply rigorous change management, perform regular backups, and conduct annual cyber security exercises.
	Network Management & Connectivity	Implement a network management framework to ensure reliable, resilient, and secure physical, wireless, and voice networks, preventing unauthorised access and monitoring for suspicious traffic.
	Information Management	Protect information against corruption, theft, loss, and unauthorised disclosure throughout all stages of the information lifecycle and in information transfer agreements.
Information Protection and Risk Management	Information Risk	Aims to establish a consistent framework for managing information risk across BT, ensuring that information risks are kept within our risk appetite through regular assessments and a systematic methodology.
	Cryptography	Deploy approved cryptographic solutions consistently across BT, manage cryptographic keys throughout their lifecycle, and implement a secure public key infrastructure (PKI) to protect critical data and operations against unauthorised access or destruction.
	Access Control	Restrict access to business applications, mobile devices, systems, and networks to authorised individuals and services for specific business purposes, as defined in a formal access control policy which implements the practice of least privilege.
	Supply Chain Management	Identify and manage information risk in relationships with external suppliers throughout the supply chain, implement a supplier security management framework, integrate security into procurement, and continuously monitor and assess supplier security arrangements.
	Cloud Services	Establish and maintain a comprehensive security management approach for acquiring and using cloud services, including necessary security arrangements and risk management practices, while communicating cloud security requirements to individuals involved in purchasing, developing, configuring, or using these services.
	Threat Protection	Implement threat protection solutions that prevent critical systems, devices, and technical security infrastructure from malware infections and other malicious attacks, while managing vulnerabilities through continuous monitoring, regular penetration tests, and up-to-date patch levels.
Threat Management and Response	Security Event and Incident Management	Record and protect important security-related events, establish a security event management lifecycle, implement a threat intelligence lifecycle, and create an information security incident management framework to identify,

	respond to, recover from, and follow up on information security incidents consistently.
Security Education and Training	Comprehensive, ongoing security education, training, and awareness program to promote and embed expected security behaviour in all individuals who have access to BT's information and systems.
Systems Development	Develop business applications and systems in accordance with an approved secure system development lifecycle (SDLC) that incorporates industry good practices and information security at each stage of the lifecycle.
Business Applications	Ensure good security practices for software acquisition, implementation of effective security controls in business applications, and management of customer access to protect information throughout its lifecycle.

4. Physical Security Standard

The Physical Security Standard covers various aspects of physical security measures required to protect BT's people, assets, and information. It includes guidelines for accessing BT premises, such as the necessity for employees and third parties to wear visible security passes and the requirement for visitors to be escorted by a host.

It also outlines requirements for physical entry controls, including the use of surveillance cameras when there is a business need or regulatory requirement, and the management of all physical access points by BT Security. Additionally, it addresses the protection of high-value equipment and infrastructure, ensuring that appropriate security controls are in place to prevent unauthorised access. The standard emphasises the importance of adhering to these security measures to maintain the safety and integrity of our operations.

Appendix D Agreement of Adherence

THIS AGREEMENT OF ADHERENCE is made on [DATE] by:

- (1) British Telecommunications Limited; and
- (2) [●] of [●] (the "**New Party**")

SUPPLEMENTAL to the Binding Corporate Rules dated [DATE] made between various BT Group Companies (the "**Rules**").

The New Party and BT Ltd agree as follows:

1. The New Party confirms that it has been supplied with and has read a copy of the Rules and covenants with each of the BT Group Companies that are parties to the Rules to observe, perform and be bound by all the terms of the Rules which are capable of applying to the New Party and which have not been performed at the date of this Agreement of Adherence, to the intent and effect that the New Party shall be deemed with effect from the date of this Agreement of Adherence to be a party to the Rules (as if named as a party to the Rules).
2. This Agreement of Adherence shall be governed by and construed in accordance with the laws of the United Kingdom and the New Party hereby submits irrevocable to the non-exclusive jurisdiction of the Courts of the United Kingdom.

In witness whereof this Agreement of Adherence has been duly executed and delivered on the day and year first written above.

Signed by the IGA Coordinator

[Signature]

.....

Director

[Signature]

.....

Director/Secretary

Signed by [**New Party**] acting by
[**name of director**] and
[**name of director or secretary**]

[Signature]

.....

Director

[Signature]

.....

Director/Secretary

Address for notices:

[●]

Address for notices:

[●]

Appendix E General Processor Requirements

When a BT Data Processor Processes Personal Data on behalf of a BT Data Controller, the BT Data Processor shall:

1. Process Personal Data only in accordance with documented instructions from the BT Data Controller. If the BT Data Processor is required by law to Process Personal Data for any other purpose, it shall inform the BT Data Controller of this requirement before the Processing, unless that law prohibits this on important grounds of public interest;
2. notify the BT Data Controller immediately if, in the BT Data Processor's opinion, an instruction for the Processing of Personal Data given by the BT Data Controller infringes the UK Data Protection Legislation;
3. taking into account the nature of the processing, assist the BT Data Controller by appropriate technical and organisational measures and in so far as it is possible, in fulfilling the BT Data Controller's obligations to respond to requests from Individuals exercising their rights under the UK Data Protection Legislation; and
4. taking into account the nature of the Processing and the information available to the Processor, assist the BT Data Controller, on reasonable request, in complying with obligations to conduct data protection impact assessments and to consult with supervisory authorities in relation to the Processing of Personal Data;
5. implement and maintain appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction, damage or theft of Personal Data and having regard to the nature of Personal Data which is to be protected. As a minimum, these should include the requirements set out in Appendix C of these Rules;
6. not transfer any Personal Data to, or process any Personal Data in, any country or territory outside the UK without the prior written consent of the BT Data Controller (and the BT Data Processor shall ensure that any sub-processor complies with the same), in which case the BT Data Processor shall assume the obligations of the Data Importer as set out in the UK Standard Contractual Clauses, unless the transfer is to an Approved Country;
7. may not give access to or transfer any Personal Data to any sub-processor, unless it has prior written consent of the BT Data Controller and a written agreement with the sub-processor which imposes (at least) the same obligations as are imposed on the BT Data Processor under this Appendix E;
8. ensure that access to Personal Data is limited to those personnel who require such access and that personnel required to access Personal Data have committed to keep Personal Data confidential and comply with the obligations set out in this Appendix E or are under an appropriate statutory obligation of confidentiality;
9. in the event that the BT Data Processor ceases to be a member of the BT Group, the BT Data Processor shall securely destroy or return personal data to the BT Data Controller and delete existing copies (unless Applicable Law requires storage of the personal data, in which case the BT Data Processor will inform the BT Data Controller thereof), unless otherwise instructed by the BT Data Controller;
10. allow the BT Data Controller and its respective auditors or authorised agents to conduct reasonable audits or inspections during the term of the processing, in accordance with BT's internal audit function as described in clause 11.1 of the Rules;
11. if the BT Data Processor becomes aware of a Personal Data Breach, the BT Data Processor shall notify the BT Data Controller without undue delay after becoming aware of such Personal Data Breach, investigate the Personal Data Breach and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach. BT Data Processor shall make reasonable efforts to assist BT Data Controller in its obligations under the UK Data Protection Legislation to notify the Information Commissioner and Individuals about such Personal Data Breach;
12. notify the BT Data Controller immediately if, in the BT Data Processor's opinion, an instruction for the Processing of Personal Data given by the BT Data Controller infringes the UK Data Protection Legislation or other applicable data protection provisions; and
13. taking into account the nature of the Processing and the information available, assist the BT Data Controller in ensuring compliance with its obligations under Article 25 of the UK GDPR (Data protection by design and by default) by implementing appropriate technical and organisational measures.

Appendix F Revision Control History

Version	Date of Change	Summary of Change
V1.1	December 2020	Adoption UK BCRs
V1.2	June 2024	Annual update including uplift against UK GDPR
V1.3	August 2024	Annual update
V1.4	December 2025	Annual update
V1.5	October 2026	General formatting changes. Updated company name from BT PLC to British Telecommunications Limited