Part A
Operative provisions

1 Definitions

1.1 In this Schedule:

Controller	has the meaning given in applicable Data Protection Laws from time to time;
Data Protection Laws	means, as binding on either party or the Services: (a) the Directive 95/46/EC (Data Protection Directive) and/or Data Protection Act 1998 or the GDPR; (b) any laws which implement any such laws; and (c) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;
Data Subject	has the meaning given in applicable Data Protection Laws from time to time;
GDPR	means the General Data Protection Regulation (EU) 2016/679;
International Organisation	has the meaning in the GDPR;
Personal Data	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data Breach	has the meaning given in the GDPR;
Processing	has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including **process**, **processed**, **processing**, and **processes** shall be construed accordingly);
Processor	has the meaning given in applicable Data Protection Laws from time to time;
Protected Data	means Personal Data received from or on behalf of the Customer in connection with the performance of FCC's obligations under this Agreement; and
Sub-Processor	means any agent, subcontractor or other third party (excluding its employees) engaged by FCC for carrying out any processing activities on behalf of the Customer in respect of the Protected Data.

2 Customer's compliance with data protection laws

The parties agree that the Customer is a Controller and that FCC is a Processor for the purposes of processing Protected Data pursuant to this Agreement. The Customer shall at all times comply with all Data Protection Laws in connection with the processing of Protected Data. The Customer shall ensure all instructions given by it to FCC in respect of Protected Data (including the terms of this Agreement) shall at all times be in accordance with Data Protection Laws.

3 Supplier's compliance with data protection laws

FCC shall process Protected Data in compliance with the obligations placed on it under Data Protection Laws and the terms of this Agreement.

4 Instructions

4.1 FCC shall only process (and shall ensure FCC Personnel only process) the Protected Data in accordance with *Section 1 of* Part B of this Schedule and this Agreement (and not otherwise unless alternative processing instructions are agreed between the parties in writing) except where otherwise required by applicable law (and shall inform the Customer of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).

4.2 If FCC believes that any instruction received by it from the Customer is likely to infringe the Data Protection Laws it shall promptly inform the Customer and be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing.

5 Security

Taking into account the state of technical development and the nature of processing, FCC shall implement and maintain the technical and organisational measures set out in *Section 2 of* Part B of this Schedule to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

6 Sub-processing and personnel

6.1 FCC shall:

6.1.1 not permit any processing of Protected Data by any agent, subcontractor or other third party (except its or its Sub-Processors' own employees in the course of their employment that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the prior specific written authorisation of the Customer;

6.1.2 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under this Schedule that is enforceable by FCC and ensure each such Sub-Processor complies with all such obligations;

6.1.3 remain fully liable to the Customer under this Agreement for all the acts and omissions of each Sub-Processor as if they were its own; and

6.1.4 ensure that all persons authorised by FCC or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.

7 List of authorised sub-processors

The Customer authorises the appointment of the Sub-Processors listed below:

Daisy Wholesale & Inform Billing

8 Assistance

8.1 FCC shall (at the Customer's cost) assist the Customer in ensuring compliance with the Customer's obligations pursuant to Articles 32 to 36 of the GDPR (and any similar obligations under applicable Data Protection Laws) taking into account the nature of the processing and the information available to FCC.

8.2 FCC shall (at the Customer's cost) taking into account the nature of the processing, assist the Customer (by appropriate technical and organisational measures), insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws) in respect of any Protected Data.

9 International transfers

FCC shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to countries outside the *United Kingdom* or to any International Organisation without the prior written consent of the Customer.

10 Audits and processing

FCC shall, in accordance with Data Protection Laws, make available to the Customer such information that is in its possession or control as is necessary to demonstrate FCC's compliance with the obligations placed on it under this Schedule and to demonstrate compliance with the obligations on each party imposed by Article 28 of the GDPR (and under any equivalent Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose (subject to a maximum of *one* audit request in any 12 month period under this paragraph 10).

11 Breach

FCC shall notify the Customer without undue delay and in writing on becoming aware of any Personal Data Breach in respect of any Protected Data.

12 Deletion/return and survival

On the end of the provision of the Services relating to the processing of Protected Data, at the Customer's cost and the Customer's option, FCC shall either return all of the Protected Data to the Customer or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires FCC to store such Protected Data. This Schedule shall survive termination or expiry of this Agreement indefinitely in the case of paragraph 12 of this Part A and until *12 months* following the earlier of the termination or expiry of this Agreement in the case of all other paragraphs and provisions of this Schedule.

Part B
Data processing and security details

Section 1—Data processing details

Processing of the Protected Data by FCC under this Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this *Section 1 of* Part B.

1 Subject-matter of processing:

Customers [and their directors/employees]

2 Duration of the processing:

The duration of the contract plus 1 year after the termination of the contract.

3 Nature and purpose of the processing:

To provide some or all of the following services to our customers:

broadband, leased line, phone lines, mobile phone, Phone Systems, SIP and Hosted VoIP, SD WAN

4 Type of Personal Data:

Full name, residential address, email address, telephone number

5 Categories of Data Subjects:

Client data, employees of client data

Commented [MB1]: I've added in Phone Systems, SIP and Hosted VoIP and SD WAN

Commented [SW2R1]: Great. Again, the items in each part of this section 1 will need to be specific to the client. So for example in relation to a mobile phone customer, the subject matter will be the directors and employees who have phones. The duration is the contract and then a period of time for retention of data thereafter. It may be there is a statutory time limit you are required to abide by. Point 3 would be to provide the mobile phone service, point 4 you may need to include bank details etc and point 5 is directors and employees.

Commented [MB3R1]: As most customers have more than one service with us, can I simply keep in all services for point 3?

Commented [SW4R1]: Yes that should be fine

Section 2—Minimum technical and organisational security measures

1 FCC shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

1.1 In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, FCC shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.

Marketing Services

With your permission and/or where permitted by law, we may also use your data for marketing purposes which may include contacting you by email, telephone and post with information, news and offers on Our services. We will not, however, send you any unsolicited marketing or spam and will take all reasonable steps to ensure that We fully protect your rights and comply with Our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.