SCHEDULE I: DATA PROTECTION SCHEDULE
VERSION 1 – EFFECTIVE FROM THE PRODUCTION DELIVERY DATE

Introduction

This **Data Protection Schedule** is a schedule to **our agreement** with **you.**

This schedule sets out the additional terms, requirements and conditions on which **we** will **process** the **Personal Data** of **your** customers contained in **switching messages** when **we** provide you with **Services.**

This schedule does not apply when **we** are the **Data Controller** of **business contact Personal Data:** the terms that apply in those circumstances are set out in **our** privacy policy available from time to time on **our** website.

When **we** provide **Services** to **you**, we deliver **switching messages** to and from **you.** To do this, **we:**

- actively access and **Process** information in the **switching message** envelope (as specified in the API), which does not contain **Personal Data**; and
- do not actively access or **Process** the **switching message** body (as specified in the API) which contains **Personal Data.**

Our hub is hosted and managed wholly within the UK. To the extent that we provide ancillary support services from outside the UK, those systems and personnel have no access to **switching messages** containing **Personal Data.**

This **Data Protection Schedule** contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) effective in the UK for contracts between controllers and processors.

AGREED TERMS

1. What do words mean in this schedule?

In this **Data Protection Schedule**, the following words have the following meanings:

Authorised Persons	the persons or categories of persons that **you** authorise to give **us** written personal data processing instructions and from whom **we** agree solely to accept such instructions, being **your** contacts recorded by **us** when you onboard with **us**

Business Purposes	the **Services** provided by **us** to **you** as described in the **agreement**
Commissioner	the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018)
Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing	have the meanings given to them in the Data Protection Legislation
Data Protection Legislation	all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party
Data Subject	the identified or identifiable living individual to whom the Personal Data relates
Personal Data	means any information relating to an identified or identifiable living individual that is processed by us on behalf of you as a result of, or in connection with, the provision of the Services under the **agreement**; an identifiable living individual is one who can be identified, directly or indirectly, in particular by

	reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual
Processing, Processes, Processed, Process	any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties
Personal Data Breach	a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data
Processor	a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the Controller
Records	has the meaning given to it in Clause 12
Term	this Data Protection Schedule's term as defined in Clause 10
UK GDPR	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018

The Annexes form part of this **Data Protection Schedule** and will have effect as if set out in full in the body of this **Data Protection Schedule**. Any reference to this **Data Protection Schedule** includes the Annexes.

A reference to writing or written includes email but not faxes.

2. Personal Data types and Processing purposes

2.1 **You** and **we** agree and acknowledge that for the purpose of the **Data Protection Legislation**:

(a) **you** are the **Controller** and **we** are the **Processor.**

(b) **you** retain control of the **Personal Data** and remain responsible for **your** compliance obligations under the **Data Protection Legislation**, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions **you** give to **us**.

(c) ANNEX A describes the subject matter, duration, nature and purpose of the processing and the **Personal Data** categories and **Data Subject** types in respect of which **we** may process the **Personal Data** to fulfil the **Business Purposes**.

3. Our obligations

3.1 **We** will only process the **Personal Data** to the extent, and in such a manner, as is necessary for the **Business Purposes** in accordance with **your** written instructions. **We** will not process the **Personal Data** for any other purpose or in a way that does not comply with this **Data Protection Schedule** or the **Data Protection Legislation**. **We** must promptly notify **you** if, in **our** opinion, **your** instructions do not comply with the **Data Protection Legislation**.

3.2 **We** must comply promptly with **your** written instructions requiring us to amend, transfer, delete or otherwise process the **Personal Data**, or to stop, mitigate or remedy any unauthorised processing.

3.3 **We** will maintain the confidentiality of the **Personal Data** and will not disclose the **Personal Data** to third-parties unless you or this **Data Protection Schedule** specifically authorises the disclosure, or as required by domestic law, court or regulator (including the **Commissioner**). If a domestic law, court or regulator (including the **Commissioner**) requires **us** to process or disclose the **Personal Data** to a third-party, **we** must first inform **you** of such legal or regulatory requirement and give **you** an opportunity to

object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

3.4 **We** will reasonably assist **you,** with meeting **your** compliance obligations under the **Data Protection Legislation**, taking into account the nature of **our** processing and the information available to **us**, including in relation to **Data Subject** rights, data protection impact assessments and reporting to and consulting with the **Commissioner** under the **Data Protection Legislation**.

3.5 **We** must notify you promptly of any changes to the **Data Protection Legislation** that may reasonably be interpreted as adversely affecting **our** performance of the **agreement** or this **Data Protection Schedule**.

4. Our employees

4.1 **We** will ensure that all of **our** employees and contractors:

(a) are informed of the confidential nature of the **Personal Data** and are bound by written confidentiality obligations and use restrictions in respect of the **Personal Data**;

(b) have undertaken training on the **Data Protection Legislation** and how it relates to their handling of the **Personal Data** and how it applies to their particular duties; and

(c) are aware both of **our** duties and their personal duties and obligations under the **Data Protection Legislation** and this **Data Protection Schedule**.

4.2 **We** will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of our employees with access to the **Personal Data**.

5. Security

5.1 **We** will implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in our **Security Policy.**

5.2 **We** will implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal data breach

6.1 **We** will within 24 hours and in any event without undue delay notify **you** in writing (and if **you** provide **us** with a nominated email address, with a copy to such nominated email address) if **we** become aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the **Personal Data**. **We** will do our best to restore such **Personal Data** at **our** expense as soon as possible.

(b) any accidental, unauthorised or unlawful processing of the **Personal Data**; or

(c) any **Personal Data Breach**.

6.2 Where **we** become aware of (a), (b) and/or (c) above, **we** will, without undue delay, also provide **you** with the following written information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope **Personal Data** and approximate number of both **Data Subjects** and the **Personal Data** records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorised or unlawful **Personal Data** processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, **we** will reasonably co-operate with **you**, in **your** handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing **you** with physical access to any facilities and operations affected;

(c) facilitating interviews with **our** employees, former employees and others involved in the matter including, but not limited to, **our** officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all **Data Protection Legislation** or as otherwise reasonably required by **you**; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the **Personal Data Breach** or accidental, unauthorised or unlawful **Personal Data** processing.

6.4 **We** will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the **Personal Data** and/or a **Personal Data Breach** without first obtaining **your** written consent, except when required to do so by law.

6.5 **We** agree that **you** have the sole right to determine:

(a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or a **Personal Data Breach** to any **Data Subjects**, the **Commissioner,** other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in **your** discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected **Data Subjects**, including the nature and extent of such remedy.

6.6 **We** will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose from **your** specific written instructions, negligence, wilful default or breach of this **Data Protection Schedule**, in which case **you** will cover all reasonable expenses.

6.7 **We** will also reimburse **you** for actual reasonable expenses that **you** incur when responding to an incident of accidental, unauthorised or unlawful processing and/or a **Personal Data Breach** to the extent that **we** caused such, including all costs of notice and any remedy as set out in Clause 6.5.

7. Cross-border transfers of personal data

7.1 **We** (and **we** will ensure that any subcontractor) will not transfer or otherwise process the **Personal Data** outside the UK without both obtaining **your** prior written consent and ensuring that such transfer is lawful.

8. Subcontractors

8.1 **We** may only authorise a third-party (subcontractor) to process the Personal Data if:

(a) **you** are provided with an opportunity to object to the appointment of each subcontractor within 20 working days after **we** supply **you** with full details in writing regarding such subcontractor;

(b) **we** enter into a written contract with the subcontractor that contains terms no less onerous as those set out in this **Data Protection Schedule** including requiring appropriate technical and organisational data security measures; and

(c) **we** maintain control over all the **Personal Data** **we** entrust to the subcontractor.

8.3 Those subcontractors approved as at the commencement of this **Data Protection Schedule** are as set out in Annex A. **We** must list all approved subcontractors in Annex A and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.4 If any subcontractor fails to fulfil its obligations under the written data protection schedule with **us** which contains terms no less onerous as those set out in this **Data Protection Schedule**, **we** remain fully liable to you for the subcontractor's performance of its data protection schedule obligations and **our** obligations to you pursuant to this **Data Protection Schedule**.

8.5 **We** agree to be deemed to control legally any **Personal Data** controlled practically by or in the possession of **our** subcontractors.

8.6 **We** will periodically audit **our** subcontractors' compliance with its obligations regarding the **Personal Data** and provide you with the audit results as part of our annual audit carried out pursuant to Clause 13.1.

9. Complaints, data subject requests and third-party rights

9.1 **We** will, at no additional cost to **you**, take such technical and organisational measures as may be appropriate, and promptly provide such information to you as you may reasonably require, to enable **you** to comply with:

(a) the rights of **Data Subjects** under the **Data Protection Legislation**, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on you by the Commissioner under the **Data Protection Legislation**.

9.2 **We** will notify you immediately in writing if **we** receive any complaint, notice or communication that relates directly or indirectly to the processing of the **Personal Data** or to either party's compliance with the **Data Protection Legislation**.

9.3 **We** will notify you within 5 business days (but will try to notify you sooner) if **we** receive a request from a **Data Subject** for access to their **Personal Data** or to exercise any of their other rights under the **Data Protection Legislation**.

9.4 **We** will give **you** **our** co-operation and assistance within a reasonable time in responding to any complaint, notice, communication or **Data Subject** request.

9.5 **We** will not disclose the **Personal Data** to any **Data Subject** or to a third-party other than in accordance with **your** written instructions, or as required by domestic law.

10. Term and termination

10.1 This **Data Protection Schedule** will remain in full force and effect so long as:

(a) the **agreement** remains in effect; or

(b) **we** retain any of the Personal Data related to the **agreement** in **our** possession or control (**Term**).

10.2 Any provision of this **Data Protection Schedule** that expressly or by implication should come into or continue in force on or after termination of the **agreement** to protect the Personal Data will remain in full force and effect.

10.3 **Our** failure to comply with the terms of this **Data Protection Schedule** is a material breach of the **agreement**. In such event, **you** may terminate any part of the **agreement** involving the processing of the **Personal Data** effective immediately on written notice to **us** without further liability or obligation.

10.4 If a change in any **Data Protection Legislation** prevents either party from fulfilling all or part of its **agreement** obligations, the parties may agree to suspend the processing of the **Personal Data** until that processing complies with the new requirements. If the parties are unable to bring the **Personal Data** processing into compliance with the **Data Protection Legislation**, either party may terminate the **agreement** on not less than 90 working days on written notice to the other party.

11. Data return and destruction

11.1 At **your** request, **we** will give **you**, or a third-party nominated in writing by **you**, a copy of or access to all or part of the **Personal Data** in **our** possession or control in the format and on the media reasonably specified by you.

11.2 On termination of the **agreement** for any reason or expiry of its term, **we** will securely delete or destroy or, if directed in writing by **you**, return and not retain, all or any of the **Personal Data** related to this **Data Protection Schedule** in **our** possession or control within 15 days, except as required by law.

11.3 If any law, regulation, or government or regulatory body requires **us** to retain any documents, materials or **Personal Data** that **we** would otherwise be required to return or destroy, **we** will notify you in writing of that retention requirement, giving details of the documents, materials or **Personal Data** that **we** must retain, the legal basis for such

retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 **We** will certify in writing to you that **we** have deleted or destroyed the **Personal Data** within 14 days after **we** complete the deletion or destruction.

12. Records

12.1 **We** will keep detailed, accurate and up-to-date written records regarding any processing of the **Personal Data**, including but not limited to, the access, control and security of the **Personal Data**, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 5.1 (**Security**).

12.2 **We** will ensure that the Records are sufficient to enable you to verify our compliance with its obligations under this **Data Protection Schedule** and the **Data Protection Legislation** and **we** will provide you with copies of the Records upon request.

12.3 **You** and **we** must review the information listed in the Annexes to this **Data Protection Schedule** at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 At least once a year, **we** will conduct audit(s) of **our** Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with **our** obligations under this **Data Protection Schedule**, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices. **We** will ensure that this is ordinarily sufficient to discharge the requirements of article 28(3)(h) of the **Data Protection Legislation.**

13.2 **We** will make all of the relevant audit reports available to **you**.

13.3 **We** will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by our management to remedy any non-compliance within a reasonable timeframe.

13.4 In accordance with the requirements of article 28(3)(h) of the **Data Protection Legislation we** will allow and contribute to audits, including inspections, conducted by **you** or auditors appointed by **you**. On the basis that **we** are owned and governed by our members (and that **you** may become a member by following the process set out in our articles of association and/or nominate candidates to become constituency directors on our board) and that our directors (appointed by our members) supervise the audit set out in Clause 13.1, **you** agree and accept that that the annual audits set out in Clause 13.1 will ordinarily be sufficient to discharge the requirements of article 28(3)(h) of the **Data Protection Legislation**, unless: (i) the audit report identifies a material concern that will not be remedied within a reasonable timeframe; (ii) otherwise required by the **Commissioner** and/or court; and/or (iii) there is a **Personal Data Breach** impacting **your Personal Data.**

14. Warranties

14.1 **We** warrant and represent that:

(a) **our** employees, subcontractors, agents and any other person or persons accessing the **Personal Data** on **our** behalf are reliable and trustworthy and have received the required training on the **Data Protection Legislation**;

(b) **we** and anyone operating on **our** behalf will process the **Personal Data** in compliance with the **Data Protection Legislation** and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) **we** have no reason to believe that the **Data Protection Legislation** prevents **us** from providing any of the **Services**; and

(d) considering the current technology environment and implementation costs, **we** will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of **Personal Data** and the loss or damage to, the **Personal Data**, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the **Personal Data** protected; and

(iii) comply with all applicable **Data Protection Legislation** and **our Security Policy**, including the security measures required in Clause 5.1.

14.2 **You** warrant and represent that **our** expected use of the **Personal Data** for the **Business Purposes** and as specifically instructed by **you** will comply with the **Data Protection Legislation.**

15. Indemnification

15.1 Subject to the limits and caps set out in paragraph 13 of the **agreed terms, we** agree to indemnify, keep indemnified and defend at **our** expense **you** against all costs, claims, damages or expenses incurred by **you** or for which you may become liable due to any failure by **us** or **our** employees, subcontractors or agents to comply with any of **our** obligations under this **Data Protection Schedule** and/or the **Data Protection Legislation**.

ANNEX A Personal Data processing purposes and details

Subject matter of processing: Delivering the content of **switching messages** to and from **you.**

Duration of Processing: The duration of **switching messages** transiting through **our hub** hosted in the UK (which may include holding and attempts to resend failed messages for a period not exceeding 14 days).

Nature of Processing: Conveyance of a **switching message** from one **hub** user to another. We will not access (nor otherwise process) the content of **switching messages.**

Business Purposes: The provision of **Services**.

Personal Data Categories: Name, address, account number, telephone number, fixed voice and broadband services received, switching date, gaining and losing provider.

Data Subject Types: Individuals contracting for fixed voice and broadband services in the UK.

Approved Subcontractors:

Tech Mahindra (operation and maintenance of the **hub**)

AWS (hosting of **hub**)