DATA PROCESSING AGREEMENT

Between

(1) You are referred to as the Controller ("you" "customer").

(2) Highspeed Office Ltd are referred to as the Processor ("us" "we" "hSo").

(hereinafter referred to as the "Parties")

Whereas

a) The Controller processes Personal Data in connection with its business activities;

b) The Processor processes Personal Data on behalf the Controller in the provision of Cloud services for the Controller as set out in the Order form;

c) The Controller wishes to engage the services of the Processor to provide Cloud services to the Controller as set out in the Order form and process Personal Data on its behalf.

Now Therefore the Parties Agree as Follows:

1. DEFINITIONS AND INTERPRETATION

Agreement: this Data Processing Agreement.

Applicable Laws: means (for so long as and to the extent that they apply to either party) the law of the European Union, the law of any member state of the European Union and/or UK Law;

Business Day: a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

Data Protection Authority: the relevant data protection authority is the Information Commissioners Office (ICO)

Data Protection Legislation: means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

2. SCOPE

2.1 The purpose of this Data Processing Agreement is to describe the work to be carried out by the Processor of Cloud Services in relation with the Agreement. This Data Processing Agreement shall be deemed to take effect from the date of an Order signed by the Parties and shall continue in full force and effect until termination of the Agreement.

2.2 This DPA is supplemental to, and forms an integral part of, the Order for services between the Parties and is effective upon an executed Order for services.

3. PROCESSING OF THE PERSONAL DATA

3.1 You are the Controller for the Personal Data and hSo is the Processor for the Personal Data. The Processor agrees to process the Personal Data only in accordance with Data Protection Legislation.

3.2 Both Parties will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Legislation.

3.3 The Parties acknowledge that the Processor may process Personal Data on behalf of the Controller during the term of this Agreement. A description of the Personal Data and the processing activities undertaken by the Processor is set out in Appendix 1.

3.4 To the extent that the Processor processes Personal Data on behalf of the Controller in connection with this Agreement, the Processor shall:

3.4.1 Solely process the Personal Data in compliance with the Controller's written instructions as set out in this Agreement (unless required by law to process personal data without such instructions) and as may be specified from time to time in writing by the Controller;

3.4.2 Notify the Controller immediately if any instructions of the Controller relating to the processing of Personal Data are unlawful;

3.4.3 Maintain a record of its processing activities in accordance with Article 30(1) of the GDPR;

3.4.4 Assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR taking into account the nature of the data processing undertaken by the Processor and the information available to the Processor, including (without limitation):

3.4.4.1 Sub-Processors

a) The Processor will not subcontract to another Processor unless instructed to do so in writing by the Controller;

b) any sub-processors engaged by the processor are subject to the same data protection obligations as the processor and that the processor remains directly liable to the controller for the performance of a sub-processor's data protection obligations;

c) the processor obtains either a prior specific authorisation or general written authorisation for any sub-processors the processor may engage to process the personal data received from the controller;

d) the Processor will ensure that obligations equivalent to the obligations set out in this clause 3 are included in all contracts between the Processor and permitted Sub-Contractors who will be processing Personal Data;

e) Ensure that its Sub-Processor shall not transfer to or access any Personal Data from a Country outside of the European Economic Area without the prior written consent of the Controller;

f) The Controller may object to the Processors use of a new sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying the Processor promptly in writing within ten (10) working days after receipt of notice by the Processor of such new appointment. Failure to object within 10 working days following Processor's notice shall be deemed to be acceptance of the new sub-processor. If a Customer reasonably objects to a new Sub-processor, the processor will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer of the services to avoid processing of personal data by the new sub-processor without unreasonably burdening the customer. If the Processor is unable to make available such change within thirty (30) days, customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those services which cannot be provided by Processor without the use of the objected-to new sub-processor, by providing written notice to Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Processor. Until a decision is made regarding the new sub-processor, processor may, at its sole discretion, temporarily suspend the Processing of the affected Personal Data and/or suspend access to the services. Customer will have no further claims against Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or this DPA in the situation described in this paragraph.

3.4.4.2 International Data Transfers

a) The Processor shall comply with the Controller's instructions in relation to transfers of Personal Data to a Country outside of the European Economic Area unless the Processor is required, pursuant to Applicable Laws, to transfer Personal Data outside the European Economic Area.

b) Transfers from the UK to other countries which have been subject to a relevant Adequacy Decision may be made without any further safeguard being necessary.

c) Transfers from the UK to other countries which have not been subject to a relevant Adequacy Decision, such transfers will be performed through an alternative recognised compliance mechanism for the lawful transfer of personal data, in compliance with article 46 of the UK GDPR. Processor will transfer Personal Data originating from the UK to countries that have not been subject to a relevant

Adequacy Decision only subject to the International Data Transfer Agreement (IDTA) or the Addendum or an alternative recognised compliance mechanism as set out by the ICO, for the lawful transfer of personal data set out in Article 46 of the UK GDPR.

3.4.4.3 Staff Confidentiality

The Processor shall ensure that any persons used by the Processor to process Personal Data are subject to obligations of confidentiality in relation to the Personal Data;

3.4.4.4 Security Measures

a) The Processor will ensure it has appropriate technical and organisational measures, that demonstrates its' ability: to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

b) The processor shall take all measures required pursuant to Article 32 of UK GDPR (Security of Processing) including but not limited to implementing appropriate technical and organisational measures to protect personal data received from the controller.

This may include the following types of measures when appropriate:

- anonymisation, pseudonymisation and encryption of personal data
- ensuring the confidentiality, integrity, availability, and resilience of processing activities
- the ability to restore personal data in a timely manner in the event of a physical or technical incident
- regular security testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure the security of processing

3.4.4.5 Data Subject Rights

a) The Processor will assist the Controller by supporting their obligations under the GDPR, insofar as possible, concerning data subjects' rights as per Chapter 3 of the GDPR;

b) The Processor shall promptly notify the Controller if it receives a request from a Data Subject (Data Subject Access Request) under any Data Protection Legislation in respect of Personal Data; and

c) Ensure that it does not respond to that request except on the documented instructions of the Controller or as required by applicable Data Protection Legislation to which the Processor is subject, in which case the Processor shall to the extent permitted by applicable Data Protection Legislation inform the Controller of that legal requirement before the Processor responds to the request; and

d) Taking into account the nature of the data processing activities undertaken by the Processor, provide assistance and co-operation (including without limitation putting in place appropriate technical and organisational measures) to enable the Controller

to fulfil its obligations to respond to requests from individuals exercising their rights under the Data Protection Legislation;

3.4.4.6 Data Breaches

The Processor shall provide information and assistance upon request to enable the Controller to notify Data Security Breaches to the Information Commissioner and / or to affected individuals and / or to any other regulators to whom the Controller is required to notify any Data Security Breaches;

3.4.4.7 Data Protection Impact Assessments

The Processor shall provide input into and carry out Data Protection Impact Assessments in relation to the Processor's data processing activities;

3.4.4.8 Deletion or Return of Data

a) Upon termination of this Agreement, at the choice of the Controller, the Processor shall delete securely or return all Personal Data to the Controller and delete all existing copies of the Personal Data unless and to the extent that the Processor is required to retain copies of the Personal Data in accordance with Applicable Laws; and

b) In the event that the Personal Data is deleted or destroyed by the Processor, the Processor shall provide the Controller with a certificate of destruction evidencing that the Personal Data has been destroyed or deleted;

3.4.4.9 Audits

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out herein.

Where the Cloud Controller audits are impractical or impose and increase risk to the Processor security, the Processor will make available independent evidence that information security is implemented and operated in accordance with the Processors information security policy.

3.4.4.10 Disclosures

The Processor shall notify the controller of any legally binding request for disclosure of Personally Identifiable Information by a law enforcement authority, unless such a disclosure is otherwise prohibited. The processor shall

a) reject any requests for PII disclosure that are not legally binding;

b) consult with the corresponding controller where legally permissible before making any PII disclosures; and

c) accept any contractually agreed requests for PII disclosure that is authorised by the corresponding controller

3.4.5 The Processor shall not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer;
b) the Data Subject has enforceable rights and effective legal remedies;
c) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
d) the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.

4. GENERAL TERMS

4.1 Breach Identification and Notification

The Processor shall notify the Controller without undue delay (and in any event within 24 hours) of becoming aware of a breach if:

4.1.1 the Processor or any Sub-Contractor engaged by, or on behalf of, the Processor suffers a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data; or

4.1.2 the Processor or any Sub-Contractor engaged by, or on behalf of, the Processor receives any data security breach notification, complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation.

And in each case the Processor shall provide full co-operation, information and assistance to the Controller in relation to any such data security breach, compliance notice or communication.

4.2 Confidentiality

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

We will notify cloud service customers of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

5. Liability

Nothing in this Agreement shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the GDPR. Furthermore, the Data Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its

obligations as a data processor under the GDPR may render it subject to the fines, penalties, and compensation requirements set out in the GDPR**.**

6. GOVERNING LAW AND JURISDICTION

This Agreement is governed by the laws of England and Wales.
This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by and shall be construed and interpreted in accordance with the laws of England and Wales, and the Parties irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales.

7. TERM AND TERMINATION

This DPA will follow the term of the Agreement and shall remain in force until such time as the Agreement is terminated (in accordance with the main contract terms) or expires. This agreement will expire at the expiry of the last provisioned service on an Order between the parties.

On termination of this Agreement for whatever reason, the Processor shall cease to process the Personal Data and Confidential Information and shall delete the data still held by the Processor and shall provide written evidence to support the deletion activity on the request of the Controller Data unless and to the extent that the Processor is required to retain copies of the Personal Data in accordance with Applicable Laws.

Termination of this Agreement shall not affect any rights or obligations of either Party which have accrued prior to the date of termination and all provisions which are expressed to, or do by implication, survive the termination of this Agreement shall remain in full force and effect.

8. NOTICES

All notices or other communications given to a Party under or in connection with this Agreement shall be in writing as set out in clause 20 of the hSo General Terms and Conditions.

We reserve the right to amend this agreement in whole or in part by notice to you in writing and/or by publishing them on our website, effective one month from the date of the amendment.

APPENDIX 1

DATA PROCESSING ACTIVITIES

DESCRIPTION OF DATA

This Appendix 1 includes the processing activities carried out by the Processor as required by Article 28(3) GDPR.

The Processor may process Customer Personal Data as necessary to technically perform the Services, these include but are not limited to the following, where applicable:

- Hosting and storage;
- Backup and disaster recovery;
- Technically improve the service;
- Service change management;
- Issue resolution;
- Providing secure, encrypted Services;
- Applying new product or system versions, patches, updates, and upgrades;
- Monitoring and testing system use and performance;
- Proactively detect and remove bugs;
- Network security purposes including incident management;
- Maintenance and performance of technical support systems and IT infrastructure;
- Migration, implementation, configuration and performance testing;
- Making product and service recommendations;
- Providing customer support; administration; transferring data, and
- Assisting with Data Subject requests (as necessary)

Personal data of all types may include: Name, Salutation, Job Title, Business Telephone Number, Business Email address, Location Address, IP address, Product details, other information as required to technically perform the services set out in the Order form.

CATEGORIES OF DATA SUBJECTS

The Controller has defined the following Data Subject categories from who the Personal Data will be collected.

- Customer;
- natural persons who are employees, contractors, agents, representatives or other business contacts of the Customer; and
- Customer's end users who are authorised by the Customer to access and use the services

LAWFUL BASIS OF DATA PROCESSING

The Controller has determined the following lawful basis to process personal data under the Data Protection Act 2018/GDPR 2016 is based on:

Consent of the data subjects, Contractual Obligation, Legal Obligation, Legitimate Interests

Cloud Services Processing Personal Data and Data Subjects

1. The Processor shall comply with any further written instructions with respect to processing by the Controller for Cloud Services.
2. Any such further instructions shall be incorporated into this Schedule.
3. The contact details of hSo's Data Protection Officer is: Karen Fisher, DataProtectionOffice@hso.co.uk

Description	**Details**
Identity of Controller for each category of Personal Data: Scope:	The Customer is the Controller and hSo is the Processor of the Personal Data. 1.For the setting up the services under the Agreement the personal data and PII scope is the business contact details of the customer. 2.For the customer data which is to be uploaded onto the hSo infrastructure (including Cloud) or transmitted over the hSo infrastructure the personal data and PII scope is the customer data uploaded onto or transmitted over the infrastructure by the Customer
Subject matter of the processing	1.The controller will provide hSo the relevant controllers business contact information set out below under the heading Type of Personal Data 2.For the customer data which is to be uploaded onto the hSo infrastructure or transmitted over the hSo infrastructure the controller will provide the relevant data onto the hSo infrastructure directly, including personal data and PII in encrypted format
Duration of the processing	The duration of the Agreement for services between the parties including any period of extension and any period required by law or regulation.
Nature and purposes of the processing	1.The operation of collecting, hosting, recording, storing and displaying Customer relevant contact information within the hSo CRM systems, hSo customer portal and other ancillary services.

	hSo will use the customer business contact information for the purpose of ensuring effective communication in providing the services set out in the Order form. Within the hSo customer portal the customer will add and amend relevant customer business contact details as appropriate for the purpose of accessing relevant customer information. 2. For the customer data which is to be uploaded onto the hSo infrastructure or transmitted over the hSo infrastructure, the operation of storing, transmitting, recording, actioning and otherwise processing the data in relation to the services provided by hSo as appropriate, which may include providing backup records of the data as appropriate per the Order form.
Type of Personal Data	1.Customer business contact name, business address and email address, business telephone number. 2. For the customer data which is to be uploaded onto the hSo infrastructure or transmitted over the hSo infrastructure, the personal data and PII is the relevant data that the customer uploads or transmits over hSo infrastructure. **Note -** it is the responsibility of the customer, and it is not the responsibility of hSo, to ensure that all personal data including personally identifiable information is encrypted by the customer at all times, including prior to and during the upload and transmission over the infrastructure
Categories of Data Subject	1.Relevant Customer Personnel as appropriate 2. For the customer data which is to be uploaded onto the hSo infrastructure or transmitted over the hSo infrastructure, data subject is relevant Customer data which contains personal data and personally identifiable information

Appendix 2

PROCESSING ACTIVITIES

To help us deliver the services, we engage with sub-processors to assist with our data processing activities. The list of sub processors hSo may share your data with include the following third parties:

www.hso.co.uk/privacypolicy/thirdparties