Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is supplemental to the Terms and Conditions for the Supply of Services (the "Agreement") between Secure Data Management Limited and the Customer.

If any terms and conditions contained herein are in conflict with the terms and conditions set forth in the Agreement, the terms and conditions set forth in this DPA shall be deemed to be the controlling terms and conditions to the extent of such conflict only. Unless specifically defined herein, all capitalised terms shall have the same meanings as are given to them in the Agreement.

The following amendments and/or additions to the Agreement are agreed.

BACKGROUND AND PURPOSE

(A) This DPA sets out the terms and conditions for the Processing of the Personal Data by Secure Data Management on behalf of the Customer under the Agreement, pursuant to which the Customer acquires the Services (as defined in the Agreement and accompanying documents) from Secure Data Management.

(B) Secure Data Management and its affiliated companies and partners act as a data processor or sub-processor ("Processor") and the Customer and its affiliated companies act as a data controller or as a data processor with respect to Personal Data, the concepts of which are further defined in the Data Protection Regulation.

(C) "Data Protection Regulation" shall mean the EU Data Protection Directive 95/46/EC including Regulation (EU) 2016/679 ("GDPR"), any United Kingdom law implementing the GDPR and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the EU (including in the event of a "no deal Brexit scenario")

(D) To the extent that the Processor Processes Personal Data, such Processing shall be governed by the Data Protection Regulation.

IT IS AGREED as follows:

1. **DEFINITIONS**

Any terms not defined in this DPA shall be given the meaning set forth in the Data Protection Regulation.

"Personal Data" shall only mean the Personal Data that is subject to the Services under the Agreement.

"Supervisory Authority" shall mean the local Data Protection Authority or any other regulatory/supervisory authority, governmental body.

"Process" or "Processing" (or any variation thereof) shall mean any operation or set of operations that is performed on Personal Data, whether or not by automatic means, such as viewing, accessing, collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

2. **SCOPE and PURPOSE; CATEGORIES of PERSONAL DATA and DATA SUBJECTS**

The purpose and subject matter of the Processing of the Personal Data by the Processor is the performance of the Services pursuant to the Agreement. The types of Personal Data and categories of Processing activities and Data Subjects covered by this DPA are further specified in APPENDIX 1. The duration of the Processing shall be the term of the Agreement, subject always to Sections 4.1.13 and 4.1.14. 2

3. **RIGHTS AND RESPONSIBILITIES OF THE CUSTOMER**

The Customer shall: (i) Process the Personal Data in compliance with the Data Protection Regulation; (ii) be authorised to give documented instructions to the Processor on the Processing of the Personal Data (including on behalf of any third party entity which is a Controller of the Personal Data), such instructions shall be binding on the Processor unless the completion of the instructions requires the provision of services under the Agreement and the Customer does not approve the corresponding service fees, or the completion of the Customer's instructions would be contrary to any Sections under this DPA; (iii) at all times retain the control and authority over the Personal Data in relation to the Processing; and (iv) at all times retain title and other rights, howsoever arising, to the Personal Data. Notwithstanding the foregoing but in respect of which the Customer hereby grants the Processor a non-exclusive, royalty free license to use, store and Process the Personal Data to the extent necessary to provide the Services. Additionally, the Customer shall be responsible for informing Secure Data Management of any updates required to APPENDIX 1.

4. **RESPONSIBILITIES AND RIGHTS OF THE PROCESSOR**

General principles applying to the processing of the Personal Data:

4.1.1 The Processor shall not use the Personal Data for any purposes other than those specified in the Agreement and this DPA.

4.1.2 The Processor shall: (i) Process the Personal Data in accordance with prevailing information management industry standards and in compliance with applicable laws and regulations; (ii) Process the Personal Data only in accordance with the documented instructions of the Customer and immediately inform the Customer if, in its opinion, a Customer instruction infringes the Data Protection Regulation or other European Union or Member State data protection provisions; (iii) ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (iv) to the extent feasible and subject to any applicable fees in the Agreement, assist the Customer in its response to rights exercised by Data Subjects or powers exercised by Supervisory Authorities under the Data Protection Regulation; (v) provide the Customer with all information necessary to demonstrate compliance with the Processor's obligations set out in this DPA and in the Data Protection Regulation; (vi) allow for and contribute to audits, including inspections, conducted by the Customer as set forth (and subject to the limitations) in Section 7 of this DPA; (vii) Process the Personal Data only during the term of this DPA as stipulated under Sections 2, 4.1.13 and 4.1.14; (viii) provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to a Supervisory Authority, in each case where these are required by the Data Protection Regulation, and solely in relation to Processing of Personal Data by the Processor on behalf of the Customer and taking into account the nature of the Processing and information available to the Processor.

4.1.3 The Processor may collect and Process contact details of the Customer employees and employee of any affiliates as a data controller for the purposes of contract and customer relationship management. The obligations on Processor set out in this DPA shall not apply to such Personal Data.

4.1.4 This DPA shall not prevent the Processor from disclosing or otherwise Processing the Personal Data as required by law, regulation or by a competent court or Supervisory Authority.

4.1.5 If Supervisory Authority or a competent court makes a request concerning the Personal Data, including a request for blocking, deleting, amending the Personal Data, delivering to them any information or executing any other actions, the Processor shall, without undue delay, inform the Customer of such requests prior to any response or other action concerning the Personal Data, or as soon as reasonably possible in case any law or regulation prescribes an immediate response to the Supervisory Authority or a 3 competent court, unless such notice to the Customer is prohibited by the respective law, regulation or warrant. The Processor may only correct, delete, amend or block the Personal Data processed on behalf of the Customer when instructed to do so by the Customer or by a competent court or Supervisory Authority or as required by law or regulation.

4.1.6 The Customer shall compensate the Processor for all reasonable costs and expenses it incurs under this DPA, unless such costs are specified as being for the Processor's account as part of the Services.

Data Security

4.1.7 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing the Processor shall implement technical and organisational measures to ensure the confidentiality, integrity, availability of the Personal Data and to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure. The Processor's security standards are incorporated in APPENDIX 2 of this DPA.

Personal Data Breach Notification

4.1.8 In the event of a "Personal Data Breach", i.e., a breach of security leading to accidental or un-lawful destruction, loss, alternation, unauthorised disclosure of, or access to, the Personal Data, the Processor shall without undue delay notify the Customer once it has a reasonable degree of certainty that a Personal Data Breach has occurred.

4.1.9 The Personal Data Breach notification shall contain at least the following (to the extent the Processor is privy to such information): a description of the nature of the Personal Data Breach including, the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned; a description of likely consequences of the Personal Data Breach; and a description of the measures taken to address the Personal Data Breach and to mitigate its possible adverse effects.

4.1.10 Where, and in so far as, it is not possible to provide the information listed in Section 4.1.9 at the same time, the information may be provided in phases without undue further delay. In such cases when the Processor cannot provide certain information listed in Section 4.1.9 to the Customer, the Processor will inform the Customer accordingly.

4.1.12 The Processor shall take reasonable steps to protect the Personal Data after having become aware of a Personal Data Breach. After having notified the Customer in accordance with Section 4.1.8 above, the Processor shall take appropriate measures to secure the Personal Data and limit any possible detrimental effect to the Data Subjects. The Processor will cooperate with the reasonable instructions of the Customer, with any third parties designated by the Customer, and with any Supervisory Authority, to respond to the Personal Data Breach.

Returning or Destruction of Personal Data

4.1.13 Upon termination/expiry of the Agreement, based on the Customer's specific instruction and subject to Processor's fees payable by the Customer (if any), the Processor shall either delete/destroy or return to the Customer or to a third party designated by the Customer all Personal Data. Any Personal Data contained within items stored by the Processor on behalf of the Controller will be returned to the Controller in accordance with an agreed exit plan, and subject to agreed exit costs, as stipulated in the Agreement. In all other cases if the Customer fails to give any instructions regarding the deletion/destruction or return of Personal Data within fifteen (15) days of the termination/expiry of the Agreement, the Processor shall send 4 a written notice to the Customer requesting to receive within 15 (fifteen) days specific instructions whether to delete/destroy or to return the data and informing about all applicable fees payable by the Customer. Should the Customer fail to provide written instructions within this timeframe and pay the applicable fees, then the Customer hereby authorises the Processor to further process/delete/destruct or return all Personal Data even after the termination of the Agreement.

4.1.14 Notwithstanding 4.1.13, the Processor shall not be in breach of its obligations with respect to the deletion of Personal Data retained on back-up tapes as long as such back-up tapes are overridden (and thereby the Personal Data deleted) in the normal course of business.

4.1.15 The Processor shall confirm on request to the Customer in writing that any deletion/destruction or return has taken place.

5. **SUBPROCESSORS (Subcontractors)**

5.1 The Customer acknowledges and authorises the Processor to engage third parties to Process the Personal Data ("Subprocessor"), which shall include (a) Processor's affiliates or parent companies; and (b) third-party Subprocessors, including Subprocessors engaged by the Processor's affiliates or parent.

5.2 The Processor shall make available to the Customer the current list of Subprocessors as part of this DPA (as detailed in APPENDIX 3) which shall include the identities of those Subprocessors, their country of location and the services they provide for the Processor.

5.3 In case of any additions or changes to APPENDIX 3 are required, the Processor shall notify the Customer by email or by making such change available to the Customer online – indicating the name, country location, and subcontracted service of the proposed new Subprocessor. Unless the Customer objects in writing within fifteen (15) days of being informed about Processor's use of a new Subprocessor, the Processor may use the new Subprocessor for the indicated data processing activities. If Customer objects within the given timeline, the Processor will use reasonable efforts to change the Services to avoid processing of the Personal Data by the "objected-to" new

Subprocessor. If the Processor is unable to implement such changes within a reasonable period of time, which shall not exceed sixty (60) days from receipt of the Customer's written objection, the Customer may, subject to the payment of any agreed termination fees, terminate within further sixty (60) days from the date of the Processor's notice the Agreement with respect only to those Services which cannot be provided by the Processor without the use of the objected Subprocessor. If the Customer fails to send such a termination notice to the Processor within this deadline, this shall be considered as a consent to the proposed sub-processing.

5.4 The Processor shall impose contractual terms on its Subprocessors which are no less protective than those set out in this DPA.

5.5 The Processor is obliged to regularly monitor the performance of its Subprocessors and it remains fully liable for the Personal Data processing activities of its Subprocessors.

6. **TRANSFER OF PERSONAL DATA**

6.1 The Processor may process Personal Data (including inventory listings about the Articles/Files/Images/Media/Deposits, but not the actual Articles/Files/ Media/Deposits on its & its affiliates' and third parties' systems outside the European Economic Area ("EEA"). The foregoing right is subject to such transfers being under the terms of the EU Commission's Standard Contractual Clauses or similar approved mechanisms such as the EU-US Privacy Shield framework ("Privacy Shield"), or the transfer 5 being to a to a country which is approved by the European Commission as ensuring an adequate level of protection. The list of approved transfers (approved subcontractors) is on APPENDIX 3 to this DPA.

6.2 For any other Processing, the Processor shall inform the Customer in advance of any transfers outside the EEA. Unless the Customer objects in writing within fifteen (15) days of being informed by the Processor to such a transfer, the Processor may proceed with such transfer, provided appropriate safeguards (EU Commission's Standard Contractual Clauses, Privacy Shield, Binding Corporate Rules) are in place, or the transfer is to a country which is approved by the European Commission as ensuring an adequate level of protection. If the Customer objects in writing within the given timeline, the Processor will use reasonable efforts to change the Services or recommend a commercially reasonable change to the Customer's use of the Services to avoid the objected-to transfer of the Personal Data. If the Processor is unable to address the Customer's concern within a reasonable period of time, which shall not exceed sixty (60) days from receipt of the Customer's written objection, the Customer may, subject to the payment of any agreed termination fees, terminate within further sixty (60) days from the date of the Processor's notice the Agreement with respect only to those Services which cannot be provided by the Processor without the transfer of the Personal Data. If the Customer fails to send such a termination notice to the Processor within this deadline, this shall be considered as an authorization to transferring Personal Data outside of the EEA.

6.3 The Data Processor has appointed a UK Data Protection Officer who is responsible for all matters related to Data Security and Processing in the UK and who will supply copies of this Data Processing Agreement (DPA), the SDM Data Protection Policy and any other related external policies related to Data Security to the Data Controller and any authorised authority on demand. Their contact details are as follows: -

i. UK Data Protection Contact Details:

Name: Nicola Peters

Position: Quality and Compliance Manager

Email: nicola.peters@securedatamgt.com

Correspondence address: Hangar 8, Aston Down Airfield, Cowcombe Lane, Stroud GL6 8HR

6.4 The Data Processor has appointed a EU Representative who is the point of contact for all matters related to Data Security and Processing of EU Data Subjects and who will supply copies of this Data Processing Agreement (DPA), the SDM Data Protection Policy and any other related external policies related to Data Security to the Data Controller and any authorised authority on demand. Their contact details are as follows

i. EU Representative Contact Details:

Name: Claire Trévien

Position: EU Representative (EU Data Protection)

Email: EU.DATA@securedatamgt.com

Correspondence address: Secure Data Management Ltd, 2 bis rue Haute, 29000 QUIMPER. FRANCE.

7. **AUDITING**

Always provided that the Processor shall not be required to provide or permit access to information concerning: (i) other Customers of the Processor; (ii) any Processor non-public external reports; and (iii) any internal reports prepared by the Processor's internal audit or compliance function, at any time during the term of this DPA, the Customer and/or a recognised, independent third party auditor appointed by the Customer shall have the right, on at least five (5) business days' notice, to perform audits and inspections of the Processor's and it's subprocessors' facilities in accordance with the Agreement. However, any audit pursuant to this DPA shall be limited to assessing the Processor's compliance with its obligations under this DPA. Except where a Personal Data Breach has occurred, no more than one such audit shall be conducted in any twelve (12) month period.

8. **LIABILITY AND INDEMNIFICATION**

8.1 Notwithstanding of any liability limitation set forth in the Agreement, in the event of any Personal Data Breach which arises directly from the Processor's illegal, unauthorised or negligent Processing of Personal Data, the Processor agrees to reimburse the Customer, to the extent required by law, on demand for the direct, verifiable, necessary and properly incurred third-party costs of the Customer in: (a) preparation and mailing of notices to such individuals to whom such notification is required by law; and (b) the provision of credit monitoring services to such individuals as required by law for a period not exceeding twelve (12) months; provided that the Customer gives the Processor reasonable prior written notice of its intent to deliver such notice.

8.2 Each party (the "Indemnifying Party") agrees to indemnify the other party (the "Indemnified Party") from and against any third-party claims from Data Subjects, provided the claim results directly and solely from any act or omission by the Indemnifying Party which is both a violation of GDPR and a material breach of this Addendum. The Indemnifying Party shall not be liable for any portion of such claim resulting from (i) Indemnified Party's violation of GDPR or this Addendum, (ii) the negligent acts or omissions of Indemnified Party, or (iii) claims which otherwise could have been avoided or mitigated through the commercially reasonable efforts of the Indemnified Party. The Indemnified Party shall grant the Indemnifying Party the option to control the defense and/or

settlement of the claim or demand and, in the event the Indemnifying Party exercises such option to control the defense/settlement, then (i) the Indemnifying Party shall not settle 6 any claim requiring any admission of fault on the part of the Indemnified Party without its prior written consent, (ii) the Indemnified Party shall have the right to participate at its own expense, in the claim or suit and (iii) the Indemnified Party shall cooperate with the Indemnifying Party as may be reasonably requested. The Indemnifying Party's sole obligation hereunder shall be to pay any judgment rendered, or settlement made, as a result of such claim or demand.

8.3 Subject to Section 8.1, in no event shall the Processor's liability under this Section 8 exceed with respect to Personal Data Breaches, the limits of liability as set out in the Agreement. The Processor will not be required to reimburse the Customer for Personal Data Breach notification costs with respect to incidents involving Personal Data that are required to be encrypted by law, regulation or prevailing industry standards.

8.4 For the avoidance of doubt, neither party shall be liable to the other party for any fines imposed by a Supervisory Authority or for damages awarded by a competent court in respect of such party's violation of the EU Data Protection Directive 95/46/EC including Regulation (EU) 2016/679 ("GDPR"), any United Kingdom law implementing the GDPR and any data protection laws substantially amending, replacing or superseding the GDPR following any exit by the United Kingdom from the EU (including in the event of a "no deal Brexit scenario") .

9. **NOTICES**

Notices regarding any dispute, claim or controversy arising out of or relating to this DPA and its appendices, or the breach, termination or validity thereof shall be deemed sufficient if made in accordance with the Agreement.

10. **TERM AND TERMINATION**

This DPA shall apply from the Effective Date and shall survive until any of the Customer's Personal Data ceases to be processed by the Processor in accordance with 4.1.13 and 4.1.14

11. **PRIOR AGREEMENTS**

This DPA supersedes and replaces any and all previous data processing agreements or data protection or privacy clauses between the parties.

12. **APPLICABLE LAW AND DISPUTE RESOLUTION**

This DPA, and any dispute, claim or controversy arising out of or relating to this DPA, or the breach, termination or validity thereof, are governed by the laws governing the Agreement without regard to its principles and rules on conflict of laws. Any dispute, controversy or claim arising out of or in connection with this DPA will be primarily sought to be resolved through negotiations between the parties or, to the extent applicable, any defined dispute resolution process contained within the Agreement.

13. **CHANGES IN DATA PROTECTION LAWS**

Each party may notify the other party in writing from time to time of any variations to this DPA which the Party reasonably considers to be necessary to address the requirements of the Data Protection Regulation or any decision of a Supervisory Authority or competent court. Any such variations shall take effect a minimum of fourteen (14) calendar days after the date such written notice is sent to the other party, unless the other party notifies the party sending the notice of any

reasonable objections within this fourteen (14) day period, in which case the parties shall co-operate in good faith to agree on the form of the variations.

APPENDIX 1

CATEGORIES of PROCESSING ACTIVITIES; PERSONAL DATA and DATA SUBJECTS

The processing activities are set forth in the Agreement and any accompanying order forms.

The Personal Data processed under this DPA may contain the following categories of Personal Data:

1. Personal master data (name, address, title, degree, date of birth);
2. Contact details (telephone number, mobile phone number, email address, fax number, address data);

iii. Contractual master data;

1. Customer history;
2. System access / usage / authorisation data;
3. Personal Data relating to financial information and/or employment relationships;

vii. Personal Data revealing racial or ethnic origin;

viii. Personal Data revealing political opinions;

1. Personal Data revealing religious or philosophical beliefs;
2. Personal Data revealing trade union membership;
3. Genetic or biometric data;

xii. Data concerning health;

xiii. Data concerning a natural person's sex life or sexual orientation; and

xiv. Personal Data relating to criminal convictions and offences.

The groups of Data Subjects who's Personal Data are processed under this DPA consist of the following:

Past and present employees; past and present contractors or consultants; agency-supplied contractors or consultants and external secondees; job applicants and candidates; students and volunteers; individuals identified by employees or retirees as beneficiaries, spouse, domestic/civil partner, dependents and emergency contacts; retirees; past and present directors and officers; shareholders; bondholders; account holders; end-users / consumers (adults, children); patients (adults, children); by-passers (CCTV cameras); and website users.

The Customer will not deliver to the Processor Personal Data outside scope indicated above or shall notify the Processor in writing about any new data type/data subject.

APPENDIX 2

MINIMUM DATA SECURITY STANDARDS

The minimum data security standards of the Processor are set out in the Information Security Manual and associated Policies that can be shared with the customer upon written request or during a pre-booked audit of the Processor.

APPENDIX 3

A sub-processor is a third-party data processor engaged by Secure Data Management Limited, including entities from within the group, who has or potentially will have access to or process service data (which may contain personal data). Further information can be found in the data processing agreement.

Sub-Processors

Secure Data Management Limited uses the following sub-processors to provide infrastructure and services to assist it in providing its services to the highest level.

Entity	**Purpose**
Microsoft Corporation (MS Office 365)	Microsoft Office 365 provides email and Internal Network services used by the processor to facilitate support and other communications with customers and the storage of Internal files
Teledata	Teledata are used by the Processor as their Cloud Hosting Provider
Base CRM	Base is a CRM tool the processor uses to store and provide quotations for prospective customers when an enquiry is made
Xero	Xero is an accounting platform used by the processor to generate customer invoices
Mailchimp Inc	Mailchimp/Mandrill is an email sending service the processor utilities for sending service and transactional emails
Recurly Inc	Recurly is used by the processor to facilitate customer subscriptions
PrintWaste Ltd	PrintWaste Ltd are one of two sub processors used to securely destroy hardcopy data on behalf of SDM.
Restore Ltd	Restore Ltd are one of two sub processors used to securely destroy hardcopy data on behalf of SDM
O'Neil Software	O'Neil software is used by the processor to store and manage customers archive information
Stripe Inc	Stripe is a PCI Level 1 compliant used by the processor for the processing, transmission and storage of customer credit card data
Hotjar Ltd	Hotjar provide marketing insights for the processor
Livedrive Internet Ltd	Livedrive is used by the processor to securely send encrypted data to the client
Zendesk Inc	Zendesk provide help desk software the processor uses to respond to customer support queries and provide our live chat service
GoCardless Ltd	GoCardless is a PCI Level 1 compliant direct debit provider the processor uses to facilitate direct debit mandates

Date of Issue and Effective Date: 10th December 2020	**Signed:** 
Date of Next Review: June 16th 2021	**Print Name: Nicola Peters** **(Quality & Compliance Manager)**
Version: 2	