Stone Computers Limited

Data Processing
and
Service Level Agreement

ONLINE VERSION

This document should be maintained under change control. This document will be updated to include all changes to data processing services being provided.

The status and update history is as follows:

Issue	DATE	STATUS	NOTES	AUTHORITY
1	16.03.18	Issued	First Release	OPs Director
2	05.07.18	Issued	Hub Storage amend	OPs Director
3	06.09.18	Issued	Third Party Transport	OPs Director

TABLE OF CONTENTS:

0: INTRODUCTION

This Data Processing Agreement & SLA is provided by Stone to ensure both parties compliance with current Data Protection Regulations and understanding of the standard service being offered.

Customers as the Data Controller, should ensure that Data Processing methodologies and controls outlined by this agreement are acceptable in meeting their requirements as the Data Controller.

Customers who wish to have their own Data Processing Agreement in place or require changes to the content of this document, should contact the Recycling Administrator named in this document or their Account Manager.

Customers satisfied that this agreement meets their requirements can acknowledge acceptance via E mail as instructed. Customer wishing to have signed copies may use the sign off sheet at the end of this document and return this via E mail to our Recycling Administrators.

If any assistance is required with this document, please contact our Recycling Admin team.

It is a requirement of the Data Protection Act 2018 / EU General Data Protection Regulations that a Data Processing contract exists between the Data Controller and Data Processor, prior to the processing of Personal Data.

1: DEFINITIONS

1.1 The terms of agreement shall apply unless specifically amended by this agreement or the context demands otherwise.

TERM	DEFINITION
Applicable Laws	means any other law or regulation that may apply to the processing of Personal Data.
Appointed Agent	means any auditor or third party, formally appointed by the Data Controller to perform a range of tasks associated with the validation of the performance of the Data Processor.
Confidential Information	means all confidential information imparted by Controller to Processor during the term of this Agreement or coming into existence because of Processor's obligations hereunder which is either marked as confidential or which ought reasonably be regarded as confidential.
Controller Data	means all data processed by the Data Processor on behalf of the Data Controller under the terms of this data processing agreement.
Data Controller	means "controller" as defined in Article 4 (7) of the GDPR.
Data Processor	means "processor" as defined in Article 4 (8) of the GDPR; "Data Subject" means "data subject" as defined in Article 4 (1) of the GDPR.
Data Subject Rights Request	means a request under Chapter 3 of GDPR which relates to the processing of Personal Data by Processor on behalf of Controller.
Personal Data Breach	means a ''Personal Data Breach'' as defined by Article 4 (12) of the GDPR.
GDPR	means the General Data Protection Regulation Directive 2016/679.
Personal Data	means "personal data" as defined by Article 4 (1) of the GDPR and which is processed by Processor on behalf of Controller
Party	''Party'' or "Parties" means a party or the parties to this Agreement.
Service	means the provision of (Description of data processing services) to Controller deemed to be the subject matter as per Article 28 GDPR.
Third Party	means a party which is not Controller or Processor or the Data Subject to whom the Personal Data relates.

In this Agreement unless otherwise expressly stated:

1.1.1. references to Clauses are to clauses of this Agreement;

1.1.2. reference to the Schedules are to the schedules to this Agreement which form part of this Agreement and are incorporated herein;

1.1.3. references to the singular include references to the plural and vice versa;

1.1.4. headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement;

1.1.5. any phrase introduced by the terms “including”, “include”, “in particular” or any similar expression are illustrative and do not limit the sense of the words preceding those terms and such terms shall be deemed to be followed by the words “without limitation”;

1.1.6. references to a statute, or any section of any statute, include any statutory amendment, modification or re-enactment and instruments and regulations under it in force from time to time;

1.1.7. references to regulatory rules include any amendments or revisions to such rules from time to time; and

1.1.8. references to regulatory authorities refer to any successor regulatory authorities.

2: SUBJECT & SCOPE

2.1 Processor processes the Controller Data exclusively on behalf of and on the instruction of Controller in accordance with Article 28 (1) GDPR (Commissioned Data Processing). Controller remains the controller for the purposes of data protection law.

2.2 Schedule 1 of the Service Level Agreement to this Agreement contains a list of which types of Controller Data the Processor may process, the nature and purpose of processing, the permitted duration of processing, and to which categories of data subjects the Controller Data relate as per Article 28 (3).

2.3 The processing of Controller Data will take place exclusively in the territory of the United Kingdom. Data processing in other countries may only take place where the Controller has provided their prior written consent and, where applicable, additionally the requirements of Article. 44 to 47 GDPR are fulfilled, or there is an exception in accordance with Article. 49 GDPR.

3: TECHNICAL & OPERATIONAL STANDARDS

3.1 Processor hereby undertakes to Controller that it will undertake the Services on behalf of Controller in accordance with this Agreement using all reasonable skill and care.

3.2 Processor hereby provides sufficient guarantees to implement appropriate technical and organisation measures in such a manner that processing meets the requirements of Article

28 (1) of GDPR. These guarantees are listed in Schedule 2 of the Service Level Agreement to this agreement.

3.3 Controller and Processor hereby acknowledge that in relation to the Personal Data and for the purposes of the Applicable Laws, Controller is the Data Controller and Processor is the Data Processor.

4: THE TERM & TERMINATION

4.1 This Agreement shall continue in full force unless or until terminated by Controller or Processor, having given 90 days termination notice to the other party.

4.2 Controller shall instruct Processor at point of termination as to its requirements for any Controller data held at that time by Processor.

4.3 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.

5: OBLIGATIONS

CONTROLLER

5.1 Controller shall provide such information as Processor may reasonably require to provide the Services outlined in Schedule 3 of the Service Level Agreement to this agreement.

5.2 Controller shall instruct Processor generally in written or text form which includes email communication. If required, Controller may also issue instructions orally or via telephone. Instructions issued orally or via telephone require, however, immediate confirmation by Controller in written or text form.

PROCESSOR

5.3 Processor undertakes to Controller that it shall process the Personal Data only on Controller's instructions as given from time to time, and in accordance with the terms of this Agreement and all Applicable Laws.

5.4 Any instructions issued by Controller to Processor shall be done so in accordance with 5.2 and shall be documented by Processor to be evidenced to Controller on request.

5.5 If Processor is of the reasonable opinion that an instruction by Controller breaches this Agreement, an earlier instruction, or applicable data protection laws, Processor must inform Controller in writing of this immediately.

5.6 Processor shall ensure that only such of its employees who may be required by Processor to assist it in meeting its obligations under this Agreement shall have access to the Personal Data. Processor shall ensure that all employees used by it to provide the Services (i) have undergone training in the laws of data protection and in the care and handling of the Personal Data in accordance with such laws, and (ii) have undergone vetting to an appropriate level.

5.7 In particular, Processor undertakes to Controller that it will not disclose the Personal Data or any part thereof to any Third Party unless and only to the extent instructed to do so in writing by Controller.

5.8 Processor undertakes to Controller that it will not export the Personal Data or any part thereof outside the European Economic Area in any circumstances other than at the specific written request of Controller. If Processor intends to transfer Controller Data to a third country or an international organisation without having been instructed to this end by Controller, Processor will inform Controller without undue delay and as soon as possible about the purpose, legal ground and affected Controller Data, to such an extent and insofar as such notification is not legally prohibited on the grounds of a substantial public interest.

5.9 For the mutual benefit of both Parties, and to ensure compliance with this Agreement and the Applicable Laws, Controller and Processor will liaise regularly, and Processor will allow its data processing facilities, procedures and documentation to be reviewed by Controller or its auditors.

5.10 If at any time Processor is unable to meet any of its obligations under this Agreement, it undertakes to inform Controller immediately by notice in writing.

5.11 Processor is not permitted to make any copies or duplicates of the Controller Data without prior written approval by Controller. This excludes copies which are necessary for the orderly performance of this agreement as well as copies which are necessary for compliance with statutory retention obligations.

5.12 Should Controller be required to provide information to a public authority or a person relating to the processing of Controller Data, or to otherwise cooperate with a public authority, Processor shall support Controller at the first request with the provision of such information or the fulfilment of other obligations to cooperate. This applies to immediate provision of all information and documents relating to technical and organisational measures taken in line with Article. 32 GDPR relating to the technical procedure for the processing of Controller Data, the sites at which Controller Data are processed, and relating to the employees involved in processing the Controller Data

5.13 Processor will support Controller in any activity, relevant to services being carried out by Processor, which Controller or appointed agents must undertake to comply with GDPR such as Data Privacy Impact Assessment and Register of Processing Activities.

5.14 Processor must have a Data Protection Officer throughout the term of this agreement and inform Controller of the contact details of this appointment. Should the Processor make any

changes to the Data Protection Officer this information must be passed onto Controller without undue delay.

5.15 Should Processor believe they do not have to appoint a Data Protection Officer this information should be passed onto Controller prior to the enactment of this agreement.

6. ASSIGNMENT & SUB CONTRACTING

6.1. Processor shall not be entitled to assign this Agreement nor all or any of its rights or obligations hereunder, without the prior written consent of Controller.

6.2. The Controller hereby consents to the use by the Processor of the services of sub contractors as set out in Schedule 5 of the Service Level Agreement to this agreement, for the purposes set out therein.

6.3. Processor shall not be entitled to sub-contract performance of its obligations hereunder without Controller's prior written consent and Processor shall, at all times, be responsible as between itself and Controller for the observance by its assignees of the obligations contained in this Agreement as if such sub-contractors were Processor.

6.4. In the event that Processor requires Controller's prior written consent in pursuance of Clause 6, Controller shall be entitled, at its discretion, to withhold such consent and prior to issuing such consent Controller may require the party that Processor proposes to sub-contract the performance (or any part thereof) of its obligations hereunder, to enter into a direct agreement relationship with Controller in respect of the processing of any Personal Data by such party.

6.5 For the assessment of such approval, Processor must provide Controller with a copy of the intended commissioned data processing agreement between Processor and the further commissioned data processor. Processor must obligate the further commissioned data processor in that written agreement in exactly the same manner as the former is obligated on the basis of this Agreement and include the requirements set out in Clause 13.

6.6 Processor is obligated to only select – and, should Controller approve, to make use of – those further commissioned data processors which offer sufficient guarantees that the appropriate technical and organisational measures will be implemented in such a manner that the processing of Controller Data takes place in accordance with the requirements of the GDPR. Processor must satisfy itself prior to the commencement of the processing of compliance with the technical and organisational measures by the further commissioned data processor and will confirm by means of a request for approval by Controller. Upon request, Processor will provide evidence to Controller to this end.

6.7 There is no right or claim to the granting of approval. The statutory liability of Processor in their capacity as commissioned data processor remains unaffected by any approval granted.

6.8 Controller must also be granted audit and examination rights in relation to sub contractors in accordance with Clause 5 of this Agreement. Controller may request from Processor information about the essential terms and conditions of the sub contractor and the implementation of the sub contractor's obligations relating to data protection, if necessary also by inspection of the relevant contractual documentation.

7. SECURITY OF PROCESSING

7.1 Processor warrants that it undertakes appropriate technical and organisational measures to ensure a suitable level of protection for the Controller Data corresponding to the risk. This must be in consideration of the state of the art, implementation costs and the type, scope, circumstances, and aims of the processing as well as the varying likelihood of occurrence and severity of the risk to the rights and freedoms of data subjects. These measures include, inter alia, the following:

a) the pseudonymisation and encryption of Controller Data;

b) the ability to permanently ensure the confidentiality, integrity and availability of the systems, services and Controller Data in connection with the processing;

c) the ability to rapidly recover the availability of the Controller Data and access to them, should a physical or technical disruption occur;

d) a process for the regular review, assessment, evaluation and evidence of the effectiveness of the technical and organisational measures for the purposes of ensuring the security of the processing.

7.2 Processor guarantees that it has, prior to the commencement of the processing of the Controller Data, provided evidence to Controller that it has taken the appropriate technical and organisational measures to protect the data which is being processed. This evidence could be the accreditation of its Data Processing Service by an industry recognised accreditation scheme. (Article 28 (5) GDPR) Processor guarantees that it will maintain these during the term of the Agreement.

7.3 Processor guarantees that it adheres to an approved code of conduct [Article 28 (5)] prior to the commencement of the agreement.

7.4 Processor guarantees that as technology and threat evolves, by means of continual assessment, the technical and organisational measures in place are assessed for appropriateness. Because of this assessment Processor is permitted to implement alternative, adequate measures, if they do not fall below the security level of the measures agreed at the start of this Agreement. Any alternative measures are subject to the prior clauses of this agreement and evidenced to Controller as per 7.1 and 7.2.

8. TRANSFER OF PERSONAL DATA

8.1 Before transferring any Personal Data to Controller, Processor will establish with Controller the appropriate method of transfer or transmission, and will securely transfer or transmit the Personal Data to Controller in line with Controller's requirements.

9. DATA SUBJECT REQUESTS

9.1. Controller shall be responsible for responding to all Data Subject Requests in accordance with Article 12. GDPR ("data subject rights") which may be received from Data Subjects to which the Personal Data relates.

9.2. Processor hereby agrees to assist Controller with all applicable Data Subject Requests which may be received from the Data Subjects to which the Personal Data relates as per Schedule 1 of the Service Level Agreement to this agreement.

9.3. If Processor receives a Data Subject Request from a Data Subject relating to the Personal Data processed on behalf of the Controller it shall immediately and without undue delay, forward it to the person nominated by Controller under schedule 4 of clause 24 of this Agreement.

9.4. Where Controller considers that it is necessary for copies of the Personal Data to be transferred to it to respond to a Data Subject Request, Controller will inform Processor that it requires copies to be transferred. Before transferring the copies, Processor will establish with Controller the appropriate method of transfer and will securely transfer the copies of the Personal Data to Controller in line with Controller's requirements, to arrive no more than 10 working days from the date of Controller's request to Processor.

10. COMPLAINTS

10.1. Controller shall be responsible for the handling of and responding to processing any complaints or expressions of dissatisfaction which may be received from the Data Subjects to which the Personal Data relates or others, in relation to the processing of the Personal Data under this Agreement.

10.2. Processor hereby agrees to assist Controller with any applicable complaints or expressions of dissatisfaction which may be received from the Data Subjects to which the Personal Data relates or others, in relation to the processing of the Personal Data under this Agreement as per Schedule 1 of the Service Level Agreement to this agreement.

10.3. If Processor receives any complaints or expressions of dissatisfaction, relating to the Personal Data processed on behalf of the Controller it shall immediately and without undue delay, forward it to the Data Protection Officer nominated by Controller in Schedule 4 of the Service Level Agreement to this agreement.

10.4. Where Controller considers that it is necessary for copies of the Personal Data to be transferred to it to allow it to respond to a complaint or expression of dissatisfaction, Controller will inform Processor that it requires copies to be transferred. Before transferring the copies, Processor will establish with Controller the appropriate method of transfer and will securely transfer the copies of the Personal Data to Controller in line with Controller's requirements, to arrive no more than 5 working days from the date of Controller's request to Processor.

11. BREACH IDENTIFICATION & NOTIFICATION

11.1. Under the context of this agreement a Data Breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

11.2. Processor will ensure that there are sufficient checks being made on processing activities to ensure that data is being protected at all time as per clause 7.

11.3. Processor will without undue delay inform Controller if the former becomes aware of an incident which under the definition of 11.1, constitutes a data breach. This communication will be made to the Data Protection Officer nominated by Controller in Schedule 4 of the Service Level Agreement to this agreement and be classed as "Initial Notification".

11.4. Controller will be responsible for informing the Local Supervisory Authority as denoted in Clause 17. This notification will be made no later than 72 hours from the "Initial Notification' as per Article 33 GDPR.

11.5. Processor must inform Controller within 24 hours of Initial Notification the following details where possible; nature of personal breach including categories and approximate number of data subjects concerned, names and contact details of the Data Protection Office or other contact point, likely consequences of personal data breach and any measures taken or proposed to be taken to mitigate the adverse effects of the data breach. Where it is not possible to provide this information in full within 24 hours, a clearly articulated plan of activities and timelines for obtaining any missing information should be submitted to Controller within the 24-hour window.

11.6. Processor will support the Controller or Controller's appointed agent, in the investigation of any data breach incident unless such activities contravene legal or agreement obligations already in place. In such situations, a written explanation supporting the Processor's position is required.

12. RETENTION & DISPOSAL OF PERSONAL DATA

12.1. Processor undertakes to retain and dispose of the Personal Data in line with the Retention and Disposal Guidelines, as contained in Schedule 6 of the Service Level Agreement to this Agreement.

13. EVIDENCE & INSPECTIONS

13.1. Processor shall provide Controller with all necessary information to prove compliance with Controller's obligations under this Agreement upon request. Upon request of Controller, Processor shall provide Controller immediately with all relevant certificates and audit reports.

13.2. Controller is entitled to receive information from the Data Protection Officer of Processor relating to all aspects regarding the processing of Controller Data, including the technical and organisational measures taken in accordance with Clause 5.

13.3. Controller or appointed agent is entitled, with reasonable notice, to enter the business premises of Processor during normal business hours (Mondays to Fridays from 09:00 until 18:00) and inspect the technical and organisational measures as well as the processes of Processor, to satisfy themselves of the compliance with the provisions of this Agreement as well as the relevant statutory data protection provisions by Processor.

13.4. Processor guarantees Controller, or appointed agent, the access rights, information rights, and inspection rights necessary for this purpose. Processor will guarantee access to the data processing facilities, files, and other documents to allow for monitoring and auditing of the relevant data processing facilities, files and other documentation relating to the processing of the Controller Data. Processor will provide Controller, or an agent appointed by the same, with all information necessary for the inspection.

13.5. Controller and Processor are subject to public audits by the competent data protection authorities. Upon request of Controller, Processor will provide the requested information to the supervisory authorities and will also grant the latter the opportunity to audit; this includes inspections of Processor by the supervisory authorities and persons appointed by them. Processor guarantees to the competent authorities in this context the necessary access rights, information rights, and inspection rights.

13.6. Processor shall hold relevant industry accreditations to evidence capabilities in their field. These are to be maintained throughout the duration of this agreement and are listed in Schedule 2 of the Service Level Agreement.

14. INDEMNITY

14.1. Processor hereby agrees to indemnify Controller up to a maximum of £5million per incident against all losses, costs, expenses, damages, liabilities, demands, claims, fines, penalties, actions or proceedings which Controller may incur arising out of any failure by Processor or its employees to comply with any of its obligations under this Agreement.

15. OWNERSHIP

15.1. All right, title and interest in the Confidential Information shall vest solely with Controller or its licensees.

16. Confidentiality

16.1. Processor shall procure that all Confidential Information disclosed to it by Controller under this Agreement or which at any time during the term of the Agreement come into Processor's knowledge, possession or control, shall be kept confidential and shall not be used for any purposes other than those required or permitted by this Agreement and shall not be disclosed to any third party except insofar as this may be required for the proper operation of this Agreement and then only under appropriate confidentiality provisions approved in writing by Controller .

16.2. Processor will ensure, pursuant to Article. 29 GDPR, that all persons under their authority process the Controller Data exclusively in accordance with this Agreement, as well as the instructions of Controller.

16.3. The obligations of confidence contained in this Clause 16 shall not prevent Processor from disclosing information to the extent required by law or for any regulatory purposes, provided that prior written notice is given to Controller of such disclosure.

16.4. The obligations of confidence contained in this Clause 16 shall not apply to any information which:

16.4.1. is or becomes generally available to the public through no act or default of Processor or its directors, employees or agents; or

16.4.2. Processor can demonstrate from its written records, prior to its receipt from Controller was in its possession and at its free lawful disposal; or

16.4.3. Processor can demonstrate from its written records, is after its receipt from Controller, generated by employees of Processor independently of, and without knowledge of, the Confidential Information; or

16.4.4. Processor can demonstrate from its written records, is subsequently disclosed to it without any obligation of confidence by a third party who has not derived it directly or indirectly from Controller.

16.5. The obligations of confidence contained in this Clause 16 shall survive the termination of this Agreement for whatever reason for a period of: (i) three (3) years following the final disclosure of the Confidential Information by Controller to Processor; or (ii) if longer, but only to the extent reasonably required, for as long as the ongoing confidentiality of the Confidential Information, or any part thereof, remains of value to Controller and or its interests.

17. NOTICES

17.1. Any notice under or in connection with this Agreement shall be in writing (but not by fax, e-mail or similar means) and shall be delivered personally, or sent by courier or by recorded or registered mail to the Processor Account Manager or Controller main contact as detailed in Schedule 4 of the Service Level Agreement to this agreement.

17.2. A notice shall become effective on the date it is delivered to the address of the recipient Party. A Party may notify the other of a change to its notice details.

17.3. Local Supervisory Authority for the purposes of this agreement is agreed to be the UK, Information Commissioners Office.

18. SEVERABILITY

18.1. Should any provision of this Agreement be held to be illegal, invalid or unenforceable in any respect by any judicial or other competent authority under the law of any jurisdiction:

18.2. If by substituting a shorter time period or more restricted application of the provision, it would be valid and enforceable, such shorter time period or more restricted application shall be substituted.

18.3. If Clause 18.1 is not applicable:

18.3.1. such provision shall, so far as it is illegal, invalid or unenforceable in any jurisdiction, be given no effect by the Parties and shall be deemed not to be included in this Agreement in that jurisdiction;

18.3.2. the other provisions of this Agreement shall be binding on the Parties in that jurisdiction as if such provision were not included herein;

18.3.3. the legality, validity and enforceability of the provision in any other jurisdiction shall not be affected or impaired; and

18.3.4. the Parties shall negotiate in good faith to agree an alternative provision in terms which as closely as possible achieve the intention of the Parties in the original provision, do not substantially impair the Parties' original interests and do not render such provisions invalid or unenforceable.

19. VARIATION

19.1. No variation or amendment to this Agreement shall bind either Party unless made in writing and signed by duly authorised officers of both Parties.

20. WAIVER & REMEDIES

20.1. A failure to exercise or any delay in exercising any right or remedy provided by this Agreement or by law does not constitute a waiver of that right or remedy or a waiver of any other rights or remedies.

21. ENTIRE AGREEMENT

21.1. This Agreement constitutes the entire Agreement and understanding of the Parties relating to its subject matter and supersedes all prior proposals, Agreements and understandings between the Parties or their advisors relating to such subject matter.

21.2. Each of the Parties hereby acknowledges and agrees that in entering into this Agreement, it does not rely on any statement, representation, warranty, undertaking, agreement or understanding of any nature whatsoever made by any person other than as expressly included in this Agreement as a warranty (a "Prior Representation") and to the extent that it is so included that Party's only remedy shall be an agreed one for breach of warranty under the terms of this Agreement for damages. To the extent that, notwithstanding the foregoing a Prior Representation has been made and relied upon by either Party, the relevant party unconditionally and irrevocably waives any claims, rights or remedies it may have in relation thereto.

21.3. Nothing in this Clause 21 or in this Agreement shall operate to limit or exclude any liability of either Party, or the remedies available to either Party for fraud, including fraudulent acts and/or fraudulent misrepresentations.

22. FURTHER ASSISTANCE

22.1. The Parties shall execute all further documents as may be reasonably necessary or desirable to give full effect to the terms of this Agreement and to protect the rights of the Parties under it.

23. GOVERNING LAW

23.1. This Agreement shall be governed in all respects by the laws of England & Wales and each Party hereby irrevocably submits for all purposes in connection with this Agreement to the exclusive jurisdiction of the English & Welsh Courts.

24. SERVICE LEVEL AGREEMENT TO THIS AGREEMENT

This document is the Service Level Agreement ('SLA') between The Customer (Controller) and Stone (Processor) providing details of agreed service provision in support of the Data Processing Agreement and outlining service requirements.

Schedule 1

Scope & Purpose of Permitted Data Processing	
Type of Controller Data	Personal Data
Data Subject Categories	Staff, Public, Customers, Students, Children
Purpose of Processing	Secure disposal of data held on IT equipment or media
Duration of Processing	Disposal completed within 25 Working Days maximum

Schedule 2

Processor Technical and Operational standards which will be maintained

Standard	Accreditation	Audit Frequency & Body
ADISA - IT Asset Disposal Standard	Certified	Assessed by ADISA Unannounced Audits x 3 in 2 Yr cycle Full Standard Audit Tri-annually
ISO27001:2013 Information Security	Certified	Assessed by NQA Annual 3 Day Audit
Cyber Essentials Information Security	Certified	Assessed by IASME Consortium Annual submission
DIPCOG MOD – IT Disposal	Approved	Assessed by MOD Unannounced Audit – random
ISO22301:2012 Business Continuity	Certified	Assessed by NQA Annual 3 Day Audit
ISO9001:2015 Quality Systems	Certified	Assessed by NQA Annual 3 Day Audit
ISO14001:2015 Environmental System	Certified	Assessed by NQA Annual 2 Day Audit

Processor Professional bodies & Code of Conduct subscriptions

Body	Details
ADISA	ADISA Membership & Council delegate Subject to the ADISA ' Code Of Conduct '

Insurance / Indemnity Cover

Insurance	Cover
Public Liability	Insurance cover £10,000,000
Professional Indemnity	Insurance cover £10,000,000
Cyber	Insurance cover £5,000,000

Schedule 3

Outline of required Processor service & description of the Stone standard recycling service.

Service Element	Description of service provision (Stone standard Service)
Administration	Online collection request system for customers Supply of collection notes & transfer of asset ownership Supply of relevant Waste transfer / Hazardous Consignment notes Co-Ordination / Agreement of collection date & site restrictions Issue of Certificate of Disposal Issue of Asset Management Report (as requested by customer) *
Transport	Secure collection / transportation of IT assets for disposal Collection drivers background checked & carrying identification Tracked vehicles, Driver panic alarms & phones, Vehicle Immobiliser & Alarm Direct return of assets to Processor facility **
Data Processing	Identification of all data bearing media collected Identification & traceability of all data bearing media throughout process Erasure of data or physical destruction of all data media collected (see table below) Validation that collection has fully completed data processing Completion of data processing within 25 working days of receipt
Asset Recycling	Refurbishment & re purposing of all viable data cleansed assets Recycling of materials from non –reusable assets

* Unless otherwise agreed the following information will be captured from data bearing assets during processing & made available for reporting as requested:
Controller asset tags / numbering
Equipment make, model, serial number and key specifications / configuration
Hard drive serial number

** Collections may be held for a short period (Max 7 Days) at a secure Hub storage facility, following collection(Dependent on UK location). Hub storage facilities will as a minimum meet the ADISA Hub Storage standards and be approved via audit by ADISA. Customer's can request to be notified if their assets are to be stored at a Hub facility. **Stone does not currently use a Hub storage location.**
Stone may engage the services of a secure logistics partner for some collections. The third party security service will is a minimum provide security at a level matching that of the Processor's.

Description of Data disposal provision (Stone standard Service)		
MEDIA TYPE	**DATA CLEANSING**	**DATA DESTRUCTION**
MAGNETIC HARD DISK DRIVES	BLANCCO OR ULTRAERASE SOFTWARE DATA ERASE * BASELINE – 1 PASS **	25MM SHREDDING (DEFAULT) 6MM ON REQUEST
SOLID STATE HARD DRIVES	BLANCCO OR ULTRAERASE SOFTWARE DATA ERASE * BASELINE – 1 PASS**	25MM SHREDDING(DEFAULT) 6MM ON REQUEST
HYBRID DISK DRIVES	-	25MM SHREDDING
SWITCHES	FACTORY RESET	25MM SHREDDING
MOBILE PHONES	SOFTWARE ERASURE	6MM SHREDDING

USB / DISKS / CARDS	-	6MM SHREDDING
MAGNETIC TAPES	ERASURE (INSURGO)	SHREDDING & INCINERATION
SERVER MOTHERBOARD	DIP SWITCH RESET	25MM SHREDDING
SIM CARDS, USB, SD CARDS	-	6MM SHREDDING

* Blancco version 6 is certified under the CPA scheme.

** Enhanced data erasure (3 passes) of Magnetic Hard Drives & Solid State Drives is available as a chargeable option when making online collection requests. Enhanced data erasure would be required to meet the criteria of HMG Information Assurance Standard No. 5

Schedule 4

Key agreement contacts:
Stone contacts Address: Granite One Hundred, Acton Gate, Stafford, Staffordshire. ST18 9AA

Stone **Data Protection Officer**	**Chris Hykin** Technical Services Director Stone Computers Ltd chris.hykin@stonegroup.co.uk
Stone **Recycling Administration**	**Becky Akers** Recycling Co-Ordinator Stone Computers Ltd becky.akers@stonegroup.co.uk DDI: 01785 786862
Stone **Accounts**	**Julie Butlin** Accounts Department Stone Computers Ltd julie.butlin@stonegroup.co.uk Tel 08448 221122 ext. 2055 Fax 08448 221123
Customer Contacts	**Please notify Stone with the details of your DPO or equivalent & main contact.**

Schedule 5

Third Parties engaged by Stone, will hold certification against the ADISA standard or have demonstrated through audit by Stone their compliance with it.
Details of current sub contractors in use for the below data processing activities will be provided on request.

Detail of Sub-Contracted Data Processing	
MEDIA TYPE	**DETAILS**
MAGNETIC TAPES	Magnetic tapes are transported by Stone for data processing at an approved third party; with specialist capabilities for this technology. Data disposal capabilities as defined in schedule 3.
MAGNETIC HARD DRIVES	Magnetic hard drives failing Stone data erasure process are transported by Stone for data processing at an approved third party; with specialist capabilities for repair and erasure of this technology. Drives failing this process are destroyed as defined in schedule 3.
TRANSPORT	Secure transportation of assets by an approved third party security service. Security service will meet as a minimum the ADISA standard for logistics.

Schedule 6

Personal data transferred to Stone for the purposes of this agreement, will be retained & disposed of as detailed.

Data retention & disposal		
DATA TYPE	**RETENTION**	**DISPOSAL**
Personal Data held on IT assets or media collected for recycling	Maximum 25 Working Days	Personal Data will be erased or media physically destroyed as detailed in Schedule 3
Personal Data of Controller contacts	7 Years	Personal Data will be erased or media physically destroyed on completion of retention period.

** A copy of Stone's Privacy Notice is available online. https://www.stonegroup.co.uk/

Schedule 7

General Service Provisions

Customer requirements:

The Customer accepts that the WEEE Directive confers upon it a Duty of Care for the handling and storage of WEEE that will afford maximum re-use potential as a complete appliance.

The Customer will also provide through the on-line collection booking system provided by Stone accurate counts of assets to be collected, in order that suitable transport be arranged and collection documentation accurately generated.

Any additions or alterations must be notified to Stone at least 24 hours prior to the scheduled collection to allow the transport proposed to be re-appraised and consequential documentation changes to be made. Additions will not be accepted without prior notification.

The Customer will collect and store notified assets for collection, in an easily accessible ground floor location that is without any access, parking or loading restrictions. Assets should be stored in a manner assisting with verification counts prior to loading.

The Customer has an obligation to verify with collection staff, the assets which have been transferred to for processing, in order that full traceability of assets can be maintained. This is of legal importance for all assets holding Personal data.
Stone accepts no liability for reported differences in asset quantities; if these were not verified and agreed at the point of collection.

A customer contact shall be provided to sign Collection & Waste Transfer documentation; which will be scanned on return to Stone and supplied to the customer contact requesting the collection.

Non-standard items (for which no category exists on the online request form) shall be notified to Stone with as much supporting information as possible to enable Stone to appraise their suitability for collection and processing, Stone will tariff them on a case-by-case basis.

The customer shall remove (if deployed) BIOS Passwords prior to collection or supply Stone with the password; in order that relevant equipment can be accessed for data erasure.

The customer shall ensure that data media such as SD Cards, CDs, USB Sticks & Hard Copy documents; which it intends to retain are removed from assets for collection. Stone will data cleanse or destroy all data bearing media (without further reference to the customer); found in the collected assets and in accordance with the Data processing agreement.

The customer shall inform Stone if it is not permissible for their collection to be made as a part of a multi-point collection. Stone will ensure that all multi-point collections are clearly segregated in transport.

The customer shall inform Stone if it is not acceptable for the collection to be made by a single driver.

The standard Stone service will normally be provided on a cost neutral basis; unless chargeable services have been requested, incurred or agreed.

The standard service requires a minimum of 25 qualifying assets. Chargeable collections can be arranged for smaller quantities on request.

Charges may be applied to agreed collections which could not be completed due to a failure by the customer. (£1.75 per mile)

Enhanced data erasure option is chargeable at £3.75 per asset.

Stone reserves the right to level charges for additional work on assets where the BIOS password has not been removed or provided by the customer.

Transfer of Ownership

Transfer of ownership of the assets for disposal shall pass to Stone at the point of collection. All data held on collected assets remains the property of the Customer; who bears legal responsibility for it as the Data Controller, as defined by Data Protection legislation.

Performance Monitoring & Review

Stone Recycling Services aim to meet performance levels as defined by the KPI's detailed below. Performance is monitored internally by Stone in order to assure its Service meets these standards and the Customer may request review meetings to discuss performance at any time.

Target Service Level Table

DESCRIPTION	KPI
All collection requests acknowledged within 48 hours of receipt.	95%
Creation of a reply to standard queries within 24 Hrs.	95%
Standard collections within 10 working days.	95%
Issue of Certificates of Disposal within 5 Working Days of receipt.	95%
Processing Completion within 25 Working Days of receipt.	95%
Issue of requested Asset Reports within 5 Working Days of processing completion.	95%

Notification of complaints or disputes about Service levels should in the first instance be raised with the Stone Account manager named in Schedule 4. Notifications can be escalated to Stone's Risk & Compliance Manager named in Schedule 4.

25: SIGNATORIES

AGREEMENT FOR THE PROCESSING OF DATA HELD ON IT ASSETS FOR RECYCLING & SERVICE LEVELS

Date of Issue: **XXX**

Commencement Date**:** **XXX**

Term: This agreement remains in force for all transactions between the named parties, until such time it is superseded by changes to it & agreed by both named parties.

This agreement between **XXX** **(the Data Controller)** and **Stone Computers Limited (the Data Processor)** details the specific requirements for processing of data held on IT assets, which under direction of the Data Controller are to be recycled .

In the existence of more than one copy, the latest version shall be deemed the current one.

We have read and agree to the terms of this Agreement:

Data Controller	**Data Processor**
SIGNED BY	**SIGNED BY**
Date	Date
……	……
Print Name	Print Name **Lawrence Richards**
Position	Position **Operations Director**
Signature	Signature
……	……
For and on behalf of **Company Name**	For and on behalf of **Stone Computers Limited**
Registered Address	**Registered Office:** **Granite One Hundred, Acton Gate,** **Stafford, Staffordshire. ST18 9AA**