Standard Contractual Clauses (processors)

For the purposes of the UK GDPR for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The **SA**/Services Agreement, referenced in this document as *the* ***SA***, refers to one or more of the following signed agreements:

- SharpSpring Partner Terms
- SharpSpring Direct Customer Terms
- Client Subscription Agreement

The Name of the data exporting organisation, the entity identified in the SA as the Customer, whose details shall be deemed incorporated into these Clauses (the "data exporter") *and operating from the address of customer identified in the SA*, reached via *telephone number of customer identified in the SA*, with *fax number of customer identified in the SA*, and contactable via the *email address of customer identified in the SA*

Other information needed to identify the customer

……
(the data **exporter**)

And

Name of the data importing organisation:

Sharpspring Inc. DBA Sharpspring Technologies Inc.

Address**:**

5001 Celebration Pointe Ave STE 410

Gainesville, Florida, USA, 32608

Tel.: **3527920277**; e-mail: **privacy@sharpspring.com**

Other information needed to identify the organisation:

……
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data'*, *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in

[1] Reference to the UK GDPR means the UK GDPR as supplemented by terms in the Data Protection Act 2018.

law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with

the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

   (b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, as identified in Appendix A to this document, or in the SA to which this document is attached.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations

performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established as identified in Appendix A to this document, or in the services agreement to which this document attached.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

As identified in the **SA.**

Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Aaron Jackson

Position: Chief Financial Officer

Address: 5001 Celebration Pointe Ave. STE 410 Gainesville, FL, USA 32608

Other information necessary in order for the contract to be binding (if any):

Signature…… Aaron Jackson

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the legal entity that has executed the Standard Contractual Clauses as a data exporter and all clients and affiliates thereof who process personal data of subjects located in the United Kingdom.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Developer and publisher of online marketing information, services and automation software which involves processing personal and customer data provided by the data exporter in accordance with the terms of the Standard Contractual Clauses (SCC) and the **SA** including all related orders between the data exporter and data importer.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The categories and types of data subjects who may be processed in accordance with the client agreement are determined and controlled by the data exporter and may include but are not limited to:

Prospects (leads), customers, contacts, website visitors, and contractors of the data exporter;

and

Prospects (leads), website visitors, employees or contractors of the data exporters' customers and clients.

Categories of data

The personal data transferred concern the following categories of data (please specify):

The categories of personal data are determined by the data exporter at its sole discretion, in accordance with the SA, and may include but are not limited to:

First and last name, contact information (e.g. email address, phone number, physical address) localization data, geographical data, device identification data, business network and experience, financial data, educational data, interests, information collected through cookies (as denoted on our Cookie Policy https://sharpspring.com/legal/sharpspring-cookie-policy/), data from exporters' connected social media accounts as authorized by the exporter, and information received from third parties (as applicable).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

The data exporter and data importer do not anticipate the transfer of special categories of data. Restrictions of this type of data are defined in the **SA** and/or Terms of Service.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Data importer will process personal data as necessary to perform applicable services in accordance with the SA. Processing operations will solely depend on the scope of data supplied by the data exporter and the exporter's configuration in the data importer's service platform. Processing operations will be performed as necessary for the data importer to provide the services agreed to in the SA for the data exporter and may include but are not limited to: collecting, tracking, recording, organizing, aggregating, storage, use, alterations, transmission, consulting, archiving and destruction.

DATA EXPORTER

Authorised Signature ……

Printed Name ……

DATA IMPORTER

Name: SharpSpring Inc DBA Sharpspring Technologies Inc.

Authorised Signature …… Aaron Jackson

Printed Name: Aaron Jackson

Company/Organization Title: Chief Financial Officer

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

This Schedule forms part of this SCC agreement and must be completed and signed by the parties

Description of the Technical and Organizational Security Measures implemented by Service Provider:

Security Policy

Policies, including those related to data privacy, security and acceptable use, are assessed and approved by SharpSpring senior management. Policies are documented and published among all relevant personnel. Employees and contracted third parties are required to comply with SharpSpring policies relevant to their scope of work.

New employees receive training on confidentiality obligations, information security, compliance, and data protection. Employees receive regular training updates, which cover SharpSpring Information Security policies and expectations. Where required, policies are supported by associated procedures, standards, and guidelines. Information Security policies are updated, as needed, to reflect changes to business objectives or risk.

Senior management performs an annual review of all Information Security policies. Information Security policies are stored, maintained, updated, and published in a centralized, online location. SharpSpring's Information Security Management System contains sections on password requirements, Internet usage, computer security, confidentiality, customer data protection, and Company data protection.

Organization of Information Security

Information Security governance and data protection compliance for the Company are the responsibility of SharpSpring's Security Manager. SharpSpring has established an Information Security team, with security responsibilities shared across various business units.

Confidentiality and nondisclosure agreements are required when sharing sensitive, proprietary, personal, or otherwise confidential information between SharpSpring and a third-party. A formal process is in place to manage third parties with access to organizational data, information systems, or data centers. All such third parties commit contractually to maintaining confidentiality of all confidential information.

Asset Management

SharpSpring assigns ownership for all information assets. SharpSpring maintains an information assets classification policy and classifies such assets in terms of its value, legal requirements, sensitivity, and criticality to the organization.

Desktops and laptops utilize encrypted storage partitions. SharpSpring maintains a data disposal and destruction policy that covers the disposal of electronic assets and associated media.

Human Resources Information Security

Security roles and responsibilities for employees are defined and documented. SharpSpring performs background screening of new hires including job history, references, and criminal checks (subject to local laws). SharpSpring requires all new employees to sign employment agreements, which include comprehensive non-disclosure and confidentiality commitments.

SharpSpring maintains a mandatory Information Security awareness and training program that includes new hire training and is repeated annually for existing employees. Information Security awareness is enhanced through regular communications using company-wide emails, as necessary. The organization maintains attendance records for any formal security awareness training sessions.

The Human Resources department notifies the Operations team about any changes in employment status and employment termination. SharpSpring maintains a documented procedure for changes in employment status and employment termination (including notification, access modification, and asset collection).

Vendor Security

Third party service providers whose services involve access to any confidential information must agree contractually to data privacy and security commitments commensurate with their access and handling of confidential information.

The SharpSpring Privacy Policy includes provisions related to the sharing of data with third party service providers and their obligations to maintain the confidentiality of that data.

Physical and Environmental Security

Physical security controls in all data centers utilized by the SharpSpring SaaS infrastructure include protection of facility perimeters using various access control measures, including biometric identification, supervised entry, 24/7/365 on-premise security teams, CCTV systems.

Access to data centers is limited to authorized employees or contractors only. Controls are in place to protect against environmental hazards at all data centers. All data center facilities have successfully been attested to SSAE 18, SOC 2 type 2, ISO 27001, or similar requirements.

Communications and Operations Management

The operation of systems and applications that support the Service is subject to documented operating procedures. The System Administration team maintains standard server configurations. Separate environments are maintained to allow for the testing of changes.

Third-party access to SharpSpring systems is regularly audited.

The organization maintains documented backup procedures. Full backups are performed regularly for all production databases. Data backups are transferred to an offsite location on a regular schedule and are stored encrypted. The physical disk arrays, which host the data, use a cipher of AES256 to store the data encrypted at rest.

All systems and network devices are synchronized to a reliable and accurate time source via the “Network Time Protocol” (NTP). All high priority event-alerting tools escalate into notifications for SharpSpring’s 24x7 incident response team, providing the System Administration team with alerts, as needed.

Access Controls

SharpSpring maintains an “Acceptable Use” policy that outlines requirements for the use of user IDs and passwords.

The organization publishes and maintains a password management standard. In general, users are asked to follow the strong password policies. Strong authentication practices (e.g., SSH keys, 2FA, IP-based restrictions) are used to control access to production and development environments.

Direct access to the “root” account on all production servers is restricted to Software Engineering and System Administration personnel as deemed necessary. All access controls are based on “least privilege” and “need to know” principles. Different roles, including read-only, limited, and administrative access, are used in the environment.

Upon notice of termination, all user access is removed in a timely fashion. All critical system access is removed immediately upon notification.

Information Systems Acquisition, Development, and Maintenance

Product features are managed through a formalized product management process. Security requirements are discussed and formulated during scoping and design discussions.

Application source code is stored in a central repository. Access to source code is limited to authorized individuals.

SharpSpring maintains a QA Department dedicated to reviewing and testing application functionality and stability. Changes to SharpSpring software are tested before production deployment. Deployment processes include unit testing at the source environment, as well as integration and functional testing within a test environment prior to implementation in production.

Information Security Incident Management

SharpSpring maintains an incident response process. Internally, SharpSpring maintains an incident response plan that is tested on a regular basis. The plan addresses specific incident response procedures, data backup procedures, roles and responsibilities, customer communication, contact strategies, and legal information flow.

The incident response plan is exercised on a regular basis, at least annually.

Business Continuity Management

For redundancy, SharpSpring utilizes database replication architectures. Database backups are stored on local disks in data centers, as well as copied to remote storage locations.

SharpSpring has implemented redundant data center infrastructure to better support high availability across the entire system. Each key service layer includes redundant components that mitigate the impact of predictable failures such as hardware problems, and also allows for capacity scaling as customer data and usage grows.

SharpSpring Application Security Features

Access to SharpSpring services requires access to a unique API key, and access to a customer's account portal requires a login and password. SharpSpring supports and encourages the use of HTTPS for all communications with our website and services.

DATA EXPORTER

Authorised Signature ……

Printed Name ……

DATA IMPORTER

Name: SharpSpring Inc DBA Sharpspring Technologies Inc.

Authorised Signature …… Aaron Jackson ……

Printed Name: Aaron Jackson

Company/Organization Title: Chief Financial Officer

25230153.2

Signature Certificate

Document Ref.: ZXUEO-SM5FF-WU6UN-DGBJB

Document signed by:

Aaron Jackson

Verified E-mail:
aaron.jackson@sharpspring.com

IP: 209.251.145.20 | Date: 17 May 2021 16:24:47 UTC

Document completed by all parties on:
17 May 2021 16:24:47 UTC