FastSpring® Data Processing Agreement for Vendors

[Last Updated: September 21, 2023]

This Data Processing Agreement ("DPA") is hereby entered into between Vendor and FastSpring at the time that Vendor agrees to the FastSpring Terms of Service for Vendors, located here. This DPA shall govern all collection and Processing of Purchaser Personal Information in relation to FastSpring's provision of services to the Vendor.

For the purposes of this Data Processing Agreement, capitalized terms shall have the meaning ascribed to them under Applicable Laws. Personal Information shall also mean Personal Data as defined under Applicable Laws. For the purposes of the CCPA, Processor shall also mean "service provider" and Controller shall mean "business."

1. **Applicable Laws**. FastSpring and Vendor agree to comply with all applicable data protection laws ("Applicable Laws") in the jurisdictions in which they operate, including but limited to: (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK Data Protection Act of 2018, as amended, the Swiss Federal Act on Data Protection of June 19, 1992, and the UK Data Protection Act, as amended; (ii) laws implemented by EU member states which contain derogations from, or exemptions or authorizations for the purposes of, the GDPR, or which are otherwise intended to supplement the GDPR; (iii) the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) (collectively referred to as "CCPA"); and (iv) any corresponding or equivalent U.S. state laws or other national laws or regulations including any amendment, update, modification to or re-enactment of such laws.
2. **Purposes of Processing**. FastSpring complies with all Applicable Laws. Personal Information will be Processed only if such Processing is based on any of the legal grounds listed in section 6(1) of the GDPR (unless an exemption applies) and in accordance with other Applicable Laws as outlined below:
    a. *Performance of a Contract*. FastSpring will Process Personal Information if it is necessary in order to enter into or perform a contract with Vendor.

b. *Legitimate Interest*. FastSpring will Process Personal Information if it is necessary for the purposes of FastSpring's legitimate interests, except where FastSpring's interests are overridden by interests or fundamental rights and freedoms that require protection of Personal Information. FastSpring's legitimate interests in Processing Personal Information include, but are not limited to, FastSpring's prevention of fraud or misuse of services, IT and network security, marketing and advertising of products sold by FastSpring, enforcement of legal claims including debt collection via out-of-court procedures, or Processing for marketing research purposes.

c. *Consent*. We may Process your Personal Information in certain circumstances with consent of the Data Subject. If we rely on consent for Processing, the Data Subject may withdraw consent at any time with effect for the future but may no longer be able to use the FastSpring Services. Where consent to the collection of Personal Information is revoked, FastSpring will stop Processing that Personal Information. For further information or to withdraw consent, please email privacy@fastspring.com.

d. *Legal Obligation*. FastSpring will Process Personal Information where we are under a legal obligation to do so, including tax compliance obligations.

3. **FastSpring's Obligations as a Data Processor**. For the following features of the FastSpring Service, FastSpring acts as a Data Processor ("Data Processor") on behalf of and in the name of the Vendor:

    a. *Pre-sale*: Purchaser completes its order on the Vendor/Data Controller's website and Vendor processes Personal Information of a Purchaser ("Purchaser Personal Information") at the Vendor's direction, including where FastSpring collects marketing consents on behalf of the Vendor

    b. *Post-purchase*: Fulfilment of the order sent by FastSpring to Purchaser.

c. Other Processing activities, including marketing activities, as directed by the Data Controller

3.1 The details of such Processing are provided at the end of this section. Each Party's obligations in relation to such Processing are described hereunder.

Personal Information remains the Vendor's property, acting as Data Controller. Therefore, the Vendor is responsible for providing Purchaser with prior information on Processing of the Personal Information during the performance of the FastSpring Service, unless otherwise agreed between the Parties.

3.2 Where FastSpring acts as a Data Processor, the following clauses apply to its Processing of Purchaser Personal Information on behalf of the Vendor:

- Taking into account the nature of the Processing and the information available to FastSpring, FastSpring will, in relation to the Purchaser Personal Information, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of GDPR and equivalent measures as required under Applicable Laws. These measures are further outlined in Appendix A to this DPA.
- FastSpring will act only on Vendor's documented instructions in relation to any Purchaser Personal Information that FastSpring Processes on Vendor's behalf and on behalf of Vendor customers, clients.
- FastSpring agrees that Vendor will continue to govern the purpose and the manner of the Processing of such data. Vendor agrees that FastSpring may Process Purchaser Personal Information collected and

retained on Vendor's behalf for FastSpring's own, limited internal business purposes.

- FastSpring will not sell or share, as those terms are defined in the CCPA, Purchaser Personal Information that it Processes on behalf of the Vendor except as otherwise allowed under this DPA.
- FastSpring will not combine Purchaser Personal Information Processed on behalf of the Vendor with Purchaser Personal Information of other Vendors to the extent such combination is prohibited by Applicable Laws.
- FastSpring will use any Personal Information Vendor submits to FastSpring only for the provision of features of the FastSpring Service to Vendor as provided in this Agreement.
- Upon Vendor's request, and in accordance with applicable laws, FastSpring will delete or return to Vendor all Personal Information.
- For the purposes of engaging vendors, suppliers, or other third parties as subprocessors of Personal Information, FastSpring will:
    - Engage sub-processors only upon Vendor's prior general written authorization. Your agreement with this Terms of Service serves as that general written authorization.
    - Require all sub-processors to adhere to the requirements of Article 32 of the GDPR and other Applicable Laws regarding the security of Processing.
    - Ensure the persons authorized to process the Personal Information are bound with confidentiality commitments or subject to an adequate legal obligation of confidentiality;
    - Provide on a reasonable basis, and pursuant to Vendor's request, all information to demonstrate the compliance with the

obligations under this Section and, where reasonable, contribute to such audits as requested by the Vendor.

- FastSpring will notify Vendor without undue delay if FastSpring becomes aware of any breach affecting Purchaser Personal Information and provide Vendor with sufficient information to allow Vendor to meet any obligations to report or inform Data Subjects, government agencies, or the appropriate national data protection authority ("National Data Protection Authority") and assist the Vendor in answering any written request received from the National Data Protection Authority or other government agency and the Purchaser after this breach.
- Cooperate with government agencies or National Data Protection Authorities, if needed;
- Inform the Vendor if it receives a request of access, modification or any other right under Applicable Laws from a Purchaser and not answer to such request without the Vendor's prior agreement;
- Immediately stop any Processing of Purchaser Personal Information from the termination or expiration of the Agreement other than the ones required under Applicable Laws, as provided otherwise herein or as agreed between the Parties.

3.3 Additional Obligations of FastSpring as a Processor. In addition to the general Data Processor provisions outlined in Section 3.2 of this DPA, for the purposes of Processing Personal Information of individuals on behalf of the Vendor in the EEA, U.K. or Switzerland, FastSpring further agrees that:

- Vendor shall be the Controller and FastSpring shall be the Processor.
- FastSpring treats all Purchaser Personal Information received from EEA member countries, the UK and Switzerland, in accordance with GDPR, the

legislation implementing GDPR in EEA member states and other relevant data protection laws.

- In relation to Purchaser Personal Information Processed in the EEA, FastSpring will assist Vendor, where possible, by appropriate technical and organizational measures, in fulfilling Vendor obligations as the Data Controller to respond to data subject requests as outlined under GDPR, Articles 12-23 (ex: requests of concerned individuals to exercise their rights; assist to Data Privacy Impact Assessment; assist to the respect of security obligations, etc.).
- Where FastSpring's Processing of Purchaser Personal Information on behalf of the Vendor requires transfer of such information to a third country or an international organization, FastSpring shall inform the Vendor of such transfer unless required to do so by Applicable Laws. In such cases, FastSpring will inform Vendor of such legal requirement before Processing, unless that law prohibits such information on the grounds of public interest.

3.4 Vendor expressly authorizes FastSpring to use one or more sub-processors listed here ("**Sub-processors**") when providing the FastSpring Service. By accepting the Terms of Service, and by extension this DPA, Vendor accepts these Sub-processors. This list of Sub-processors may be updated from time-to-time. It is the responsibility of Vendor to check the list for the most up-to-date listing of Sub-processors. FastSpring will allow Vendor the opportunity to reasonably object to the appointment of a subcontractor if such objection is for legitimate and business-related reasons (i.e. competitor, provider with whom Vendor has an ongoing dispute). Objections must be sent in writing to FastSpring at 801 Garden Street, Suite 201, Santa Barbara, CA 93101 USA. If no written objection is made by Vendor within ten (10) days following an update to the list of Sub-processors, Vendor is deemed to have accepted the new Subprocessor(s). If Vendor refuses a Sub-processor, FastSpring may apply to the Vendor a

different price than the one initially agreed on to accommodate for any change to FastSpring's use of such Sub-processors or may terminate the Agreement without any liability to FastSpring.

3.5 Description of the Processing:

- Purpose of the Processing: Pre-sale, abandonment, post purchase
- Term of the Processing: The term of the Processing corresponds to the duration of the Agreement
- Nature of the Processing: FastSpring acts as the Vendor and merchant of record of the Vendor's Products under the Agreement and processes the Purchaser`s payments for the Vendor`s Products.
- Categories of Personal Information: First name; last name; email address; and unique user code
- Categories of Data Subject: Prospects and Purchasers 4.

4. **FastSpring's Obligations as a Joint Controller**. FastSpring acts as a joint controller ("J**oint Controller**") with the Vendor of Purchaser Personal Information where each Joint Controller directs its own Processing of such Personal Information, including data collection and Processing related to the payment by a Purchaser of Vendor Products.

4.1 Where FastSpring and Vendor act as Joint Controllers, each agrees that each Joint Controller:

- Will implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and required under any other Applicable Laws;
- Will implement internal rules to regulate the various obligations imposed by Applicable Laws;

- Will carry out, if required, all the necessary formalities before the competent supervisory authorities;
- Will keep a written record of the Processing carried out under the Agreement;
- Will appoint a Personal Data Protection Officer, if required by Applicable Laws;
- Will implement measures that comply, in particular, with the principles of privacy by design and protection of privacy by default as required by Applicable Laws;
- Will determine its own purposes and manner of Processing Purchaser Personal Information and each is responsible for providing appropriate notice to Purchasers regarding its data protection practices;
- Will treat Purchaser Personal Information received from European Union (EU) member countries, the U.K. and Switzerland, in accordance with GDPR and the legislation implementing GDPR in EU member states;
- Will assist the other with data subject requests, including access and deletion, where appropriate and required by Applicable Laws;
- Will notify the other without undue delay of any breach affecting Purchaser Personal Information and coordinate with the other Party to provide notice of the breach to the national supervisory authority(ies) and/or the data subjects, within 72 (seventy-two) hours; and, where appropriate, to take the necessary steps to mitigate the said data breach;
- Will ensure that the appropriate measures are implemented in case the Personal Information is transferred to a third party, including Sub-processor (execution of standard contractual clauses, data Processing agreement that includes the requirement that Sub-processors adhere to the same or similar protections as are outlined in this DPA);

- Will retain the Personal Information for no longer than is necessary for the purposes for which the Personal Information are processed;
- Will cooperate and reply to any request for information received by either party from a government agency or competent National Data Protection Authority; and
- When Processing EEA, Swiss or U.K. Personal Information, will consult the competent National Data Protection Authority prior to Processing when a privacy impact assessment indicates that the Processing would result in a high risk if the concerned Party does not implement measures to mitigate the risk.

Regarding the relationship with Purchaser and more generally Data Subjects, as defined by Applicable Laws, FastSpring will inform them via its Privacy Statement. Vendor acknowledges that it complies with the requirements of Applicable Laws. In case Vendor receives any request for access from a Data Subject or to exercise any other right granted under the applicable data protection laws for a Processing for which the Parties act as Data Controller, it must inform FastSpring without delay and the Parties will agree on how to answer to it.

5. **FastSpring's Obligations as a Controller**. For the Processing of Personal Information of Vendor's employees and staff, FastSpring acts as a Data Controller and therefore process the Personal Information for the purposes of assisting Vendor, following-up for the different and various requests, as well as maintenance and support as part of the FastSpring Service. FastSpring provides the relevant information on the Processing of Vendor's employees their Personal Information via its privacy statement available on its Website.

6. **EU-US Cross-Border Data Transfers**.

6.1 U.S. Data Privacy Framework (EU-U.S. DPF) Compliance. FastSpring complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK

Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. FastSpring has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. FastSpring has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

In compliance with the EU-U.S. DPF Principles, FastSpring commits to resolve complaints about our collection or use of Data Subjects' Personal Information transferred to the United States pursuant to the DPF Principles. European Union individuals with DPF inquiries or complaints should first contact FastSpring at privacy@fastspring.com. FastSpring has further committed to refer unresolved privacy complaints under the DPF Principles to an independent dispute resolution mechanism, Data Privacy Framework Services, operated by BBB National Programs. If a Data Subject does not receive timely acknowledgment of their complaint, or if their complaint is not satisfactorily addressed, they may visit https://bbbprograms.org/programs/all-programs/dpfconsumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to Data Subjects.

If a DPF complaint cannot be resolved through the above channels, under certain conditions, a Data Subject may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See

https://dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset35584=2.

As explained here we sometimes provide Personal Information to third parties to perform services on our behalf. If we transfer Personal Information received under the EU-U.S. DPF to a third party, the third party's access, use, and disclosure of the Personal Information must also be in compliance with our EU-U.S. DPF obligations. Therefore, third parties that use our products explicitly agree to abide by the EU-U.S. DPF or otherwise agree to execute the Standard Contractual Clauses issued by the European Commission for the purposes of transferring Personal Information from the EU to non-adequate countries outside the EU.

6.2 Standard Contractual Clauses. Where the EU-U.S. DPF is not applicable, FastSpring executes the Standard Contractual Clauses for the purposes of lawful transfer of personal data as set out in European Commission Decision (EU) 2021/914 of 4 June 2021, as well as the UK International Data Transfer Addendum to the EU Standard Contractual Clauses as issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 (as applicable to any transfers from the UK to nonadequate third countries). Such transfers shall be executed as follows:

- **Cross-Border Data Transfers Where FastSpring is a Controller.** FastSpring and FastSpring B.V., acting as a Joint Controllers, have executed Controller-to Controller Standard Contractual Clauses in accordance with Decision 2021/914/EC to facilitate the transfer of Personal Information collected in the EEA and Switzerland, as well as the appropriate International Data Transfer Agreement for transfers of UK data, to the United States. This agreement applies to all Vendor Personal Information that is transferred by FastSpring from the EEA to the United States where FastSpring acts as a Controller of such data.

- **Cross-Border Data Transfers Where FastSpring is a Processor.** Where FastSpring acts as a Data Processor and Vendor is located in the EEA, or Switzerland, Vendor agrees to execute Controller-to-Processor Standard Contractual Clauses. Where FastSpring acts as a Data Processor and Vendor is located in the UK, Vendor agrees to execute UK-specific Standard Contractual Clauses. To execute the Standard Contractual Clauses, Vendor should review them [here] and select the appropriate option when prompted.

APPENDIX A: SECURITY

FastSpring ("FastSpring", "we", or "us") implements the following security measures on all Personal Information processed in relation to its Services:

1. We implement appropriate organization, technical and administrative controls for all personal data that we Process.
2. We implement logical access security software, infrastructure, and architectures over protected information assets to protect them from security events.
3. Prior to issuing system credentials and granting system access, we register and authorize new internal and external users. We remove user system credentials when user access is no longer authorized.
4. We encrypt or pseudonymize Personal Information where possible to protect the data that we Process. Where encryption or pseudonymization are not possible, we implement alternative, equivalent controls to protect the data.
5. We restrict access to all Personal Information to only those employees or Subprocessors who have a need to know or access the data.
6. We restrict physical access to its facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel.

7. We implement logical access security measures to protect against threats from sources outside its system boundaries.
8. We restrict the transmission, movement, and removal of information to authorized internal and external users and processes, and protect it during transmission, movement, or removal.
9. We implement controls to prevent or detect and act upon the introduction of unauthorized or malicious software.
10. We monitor system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting our ability to meet our objectives; anomalies are analyzed to determine whether they represent security events.
11. We respond to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
12. We identify, develop, and implement activities to recover from identified security incidents.
13. We assess and manage risks associated with our vendors and business partners and execute required agreements and data transfer provisions where required by applicable law.
14. We delete or destroys data in accordance with our internal records retention policies or as soon as no longer needed for business purposes.
15. We require our Sub-processors to implement security measures at least as strict as provided in this Appendix.