Notice: The Chargify service does not include any data subject notice or consent process for compliance with Customer's data controller obligations that might be required under applicable law. Customer is responsible for meeting its legal obligations prior to enabling any feature of the Chargify services that permits a data subject to communicate personal information directly to the Chargify service platform or the payment process.

DATA PRIVACY AND PROCESSING ADDENDUM

This Data Privacy and Processing Addendum (this "**Addendum**") is an addendum to the Service Terms at https://www.chargify.com/service-terms, as it may be updated from time to time, or other agreement between Chargify LLC ("**Chargify**") and the Chargify customer (the "**Customer**") for Chargify's services (the "**Services Agreement**").

1. Definitions. The following words have the meaning stated when used in this Addendum. Capitalized terms not otherwise defined in this Addendum have the meanings stated in the Services Agreement.

applicable law means (i) laws generally applicable to the processing of personal data in the United States and each State of the United States including, without limitation, the CCPA, and (ii) if applicable, the european privacy laws;

CCPA means the California Consumer Privacy Act of 2018;

data subject means an individual natural person that is identified or identifiable by means of the personal data and where applicable law applies to a business, the business that is identified or identifiable by means of the personal data;

disclose means to disclose or give access to;

european privacy laws means the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"), (ii) the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, (iii) applicable national implementations of (i) and (ii), (iii) Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance, and (iv) in respect of the United Kingdom the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and any applicable national legislation that replaces or converts in domestic law the GDPR including the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) or any other law relating to data and privacy as a consequence of the UK leaving the European Union; (in each case, as may be amended, superseded or replaced);

law means statutes, regulations, executive orders, and other rules issued by a government office or agency that have binding legal force;

personal data means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that Chargify will process or have access to as part of providing the Services, including any such information that is created by means of the Services. Personal data includes “personal data” at that term is defined in the GDPR and “personal information” as that term is defined in the CCPA;

personnel means the Customer’s employees, agents and individual contractors under the direct control of the Customer including any subscriber;

process when used with respect to personal data means: (i) to record, store, organize, structure, analyze, query, modify, combine, encrypt, display, disclose, transmit, receive, render unusable, or destroy, by automated means or otherwise, (ii) to provide cloud or other remote technology hosting services for applications or services that do any of the foregoing, and (iii) any other use or activity that is defined or understood to be processing under applicable law. The terms process, processing and their variants have the meanings defined in the GDPR;

security event means any of the following: (i) unauthorized processing or other use or disclosure of personal data, (ii) unauthorized access to or acquisition of personal data or the systems on which personal data is processed, (ii) any significant corruption or loss of personal data that Chargify is unable to repair within a minimal period of time, (iii) any event that has or is reasonably likely to significantly disrupt the processing of the personal data as contemplated by the Services Agreement, and (iv) any material unsuccessful attempt to gain unauthorized access to, or to destroy or corrupt, the personal data, but not including any routine, unsuccessful events such as pings, port scans, blocked malware, failed log in attempts, or denial of service attacks;

sensitive personal data means (i) information regarding an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, sex life, or sexual orientation, (ii) all or part of a social security number, passport number, driver's license number, or similar identifier, (iii) genetic data, biometric data (where used for identification purposes), and health information, (iv) account passwords or other credentials other than as needed to use the Chargify Services, (v) date of birth, (vi) criminal offence history, (vii) mother's maiden name, and (viii) any other information that is a special category data as defined in the GDPR;

standard contractual clauses or **SCCs** means the EU’s approved Standard Contractual Clauses further to the EU Commission’s Decision C(2010)593 as set out at Schedule 1 as amended and updated from time to time;

sub-processor and **sub-processor agreement** have the meaning given in Section 4 (Disclosure to Third Parties) below;

subscriber means an individual who the Customer bills for the Customer’s subscription product or service using Chargify’s services;

third party means any natural person or legal person other than Chargify, Customer, or either of their personnel.

2. General. As between Chargify and Customer: (i) Customer controls the purpose and means of processing of personal data, and is the "controller" under the GDPR, "data exporter" under the SCCs and the "business" under the CCPA, and (ii) Chargify is authorized to process the personal data only as instructed by Customer including as described in the Services Agreement between Chargify and Customer and this DPA, and is the "processor" under the GDPR, "data importer" under the SCCs and the "service provider" under the CCPA. Chargify shall comply with the requirements stated in this Addendum, and any additional or more stringent requirements or restrictions under applicable law. On Customer's request Chargify shall execute one or more additional data transfer and processing agreements in a form required or recognized under applicable law for international transfers of personal data, to include any standard clauses published pursuant to European privacy laws, such as the SCCs adopted by the European Commission as amended from time to time.

3. Permitted Use and Disclosure. Chargify shall not process personal data except as follows: (i) as necessary to provide the Services in accordance with the Services Agreement, subject to Section 4 (Disclosure to Third Parties), (ii) as required by applicable law, subject to Subsection 4 (Legally Required Disclosure), and (iii) as necessary to comply with legal requirements for records retention or for internal administrative purposes related to the provision of the Services, except to the extent such processing would violate restrictions under applicable law. For clarity, Chargify may not sell the personal data as that term is used in the CCPA, and may not aggregate the personal data with other data, or process, access, or use the personal data for any purpose not expressly authorized above.

4. Disclosure to Third Parties.

4.1 Disclosure to Sub-processors. Chargify shall maintain a list of sub-processors on its website (https://www.chargify.com/privacy-policy/#service-providers). Customer has consented to the use of the sub-processors identified in the Privacy Policy. Chargify may disclose Customer's personal data to a permitted subcontractor (a "sub-processor") as necessary for the sub-processor to provide the subcontracted part of the Services, provided that: (i) Chargify has conducted appropriate due diligence to confirm that the sub-processor is capable of providing the level of protection for personal data that is required by the Services Agreement and this Addendum, (ii) the sub- processor is subject to written obligations to protect the personal data that are substantially similar and at least as stringent as those stated in this Addendum, including all notice, security and, subject to the limitations set out at section 7, audit terms (each a "sub-processor agreement"), (iii) the sub-processor is required to comply with the same obligations of Chargify stated in the Addendum as to any engagement with another processor. Chargify shall be responsible for the acts and omissions of each sub-processor in violation of this Addendum to the same extent as for Chargify's own acts and omissions. If Customer reasonably objects to a sub-processor added after the effective date of this Addendum, Chargify shall not use the sub-processor to process Customer's personal data, or if that is not commercially feasible, shall permit Customer to terminate the Services Agreement without liability.

4.2 Legally Required Disclosures. Chargify may disclose personal data as required by a subpoena or other compulsory legal process provided that: (i) it gives Customer as much advance notice of the disclosure as is reasonably practical under the circumstances (unless notice is prohibited by law), (ii) it discloses only the personal data that it is legally compelled to disclose, in the reasoned, written opinion of Chargify's counsel, and (iii) it cooperates, at Customer's expense, with Customer's reasonable requests to avoid or limit disclosure, or if Chargify is not permitted to give notice of the disclosure, it uses reasonable efforts to challenge or narrow the requirement in accordance with applicable law.

4.3 Requests from Data Subjects. Chargify shall promptly notify Customer if Chargify receives a request from a data subject to disclose, provide a copy, modify, block, or take any other action with respect to the personal data, unless notice is prohibited by applicable law. Chargify shall not independently take any action in response to a request from a data subject without Customer's prior written instruction. Chargify shall cooperate with Customer's reasonable requests for access to personal data and other information and assistance as necessary to respond to a request or complaint by a data subject.

5. Protection of Personal Data. Chargify shall protect the personal data from unauthorized access or acquisition, use, disclosure, loss, corruption, alteration and unavailability using those physical, technical, organizational, and administrative safeguards described below. Chargify will require its sub-processors to use safeguards at least as protective of the personal data as the safeguards applicable to Chargify.

5.1 PCI DSS. Chargify shall comply with the Payment Card Industry Data Security Standards, version 3.2, Level 1 ("PCI DSS"). Chargify shall obtain an annual audit of its compliance with PCI DSS by a Qualified Security Assessor Company and, on Customers' written request, shall provide its most recent PCI DSS audit report.

5.2 SOC 1. Chargify shall implement and maintain the controls described in its Report on Controls that is part of an annual SSAE-16 SOC 1, Type 2 audit report (the "SOC 1 Report"). On Customers' written request, Chargify shall provide its most recent SOC 1 Report. If the SOC 1 Report describes any exceptions, Chargify shall provide a statement addressing its corrective action plan for each exception, including a timeline for the implementation of the corrective action plan.

6. Cross-Border Transfer of Personal Data. The Parties contemplate that Customer will transfer the personal data covered by this DPA to Chargify's services environment located in the United States. Transfer to and from the U.S. is made via global networks managed by Chargify's content management sub-processors and may entail temporary storage outside of the U.S. If the Customer's personal data originates from an EU data subject, the following additional terms apply to personal data covered by the GDPR: (i) Customer is the "exporter" and Chargify is the "importer" of the personal data transferred to the United States, (ii) the SCCs are attached to this DPA as Schedule 1 and are automatically incorporated in this DPA by this reference, (iii) if there is a conflict between the SCCs and the main terms of this DPA, the SCCs shall control, and (iv) Customer represents and warrants to Chargify that the transfer of the personal data of its personnel and that of any subscriber is permitted in accordance with applicable law.

7. Notice of Security Event. Chargify shall provide prompt notice to Customer's technical and account contacts using those means established for routine account-related communications if Chargify opens an "incident" or otherwise begins a formal process to investigate a suspected security event. Chargify shall provide notice as provided in Section 13.2 (Notices) without undue delay and all events within forty-eight (48) hours of discovering that a security event has occurred. A security event is "discovered" under this Section at the time it is actually discovered. Chargify's notice shall include the following information to the extent it is reasonably available to Chargify at the time of the notice, and Chargify shall update its notice as additional information becomes reasonably available: (i) the dates and times of the security event, (ii) the facts that underlie the discovery of the security event, or the decision to begin an investigation into a suspected security event, as applicable, (iii) a description of the personal data involved in the security event, either specifically, or by reference to the data set(s), and (iv) the measures planned or underway to remedy or mitigate the vulnerability giving rise to the security event. Chargify shall promptly provide other information regarding the security event or suspected security event that Customer may reasonably request. Where a security event was caused by a sub-processor engaged by Chargify, Chargify shall use all reasonable endeavours to facilitate the full cooperation of its sub-processor with Customer, and upon written request, shall use commercially reasonable efforts to facilitate Customer's, its independent third-party auditor or a regulator's audit and review of the sub-processor's information security program, data processing facilities, and data protection compliance program. In the event Chargify is unable to provide onsite inspection or other rights with regard to sub-processors despite using commercially reasonable efforts, Customer may immediately suspend the processing of any personal data, and have the right to terminate Services Agreement without liability besides for amounts due and owing.

8. Mitigation/Investigation/Remediation. Chargify shall take those measures available, including reasonable measures requested by Customer, to address a vulnerability giving rise to a successful security event, both to mitigate the harm resulting from the security event and to prevent similar occurrences in the future. Chargify shall cooperate with Customer's reasonable requests in connection with the investigation and analysis of the security event, including a request to use a third- party investigation and forensics service. Chargify shall retain all information that could constitute evidence in a legal action arising from the security event and shall provide the information to Customer on Customer's request. Except to the extent required by law in the written and reasonable opinion of Chargify's counsel, Chargify shall not disclose to any person the existence of a security event or suspected security event or any related investigation without Customer's prior written consent.

9. Cooperation. Chargify shall cooperate with Customer's reasonable requests information and assistance in connection with: (i) Customer's internal security and privacy assessments, and (ii) any audits or verifications of Customer's privacy and security policies and practices by Customer's customers, regulators, or other stakeholders.

10. Business Continuity Plan. Chargify shall maintain a written business continuity/disaster recovery plan (a "BCP") to enable Chargify to timely recover and resume its operations in the event of a disruptive event, including an event that would constitute "force majeure" event as described in the Services Agreement. Chargify shall test its BCP at least annually, in accordance with the terms of the Plan. On Customer's request, Chargify will provide a summary of its BCP, or will provide Customer and its auditors with controlled access to the full BCP, provided that the auditors are subject to confidentiality terms at least as stringent as those stated in the Agreement.

11. Records and Audit. Chargify shall keep reasonable records to evidence its compliance with this Addendum, and shall preserve the records for at least two (2) years from the date of the events reflected in the records. Chargify shall subject to section 7 regarding sub-processors, provide Customer, its independent third-party auditor or a regulator with access to its relevant records, systems, facilities and personnel for the purpose of auditing or verifying compliance with this Addendum, provided that any such audit or verification shall be performed on reasonable advance notice and shall not unduly disrupt Chargify's operations. If any audit or verification reveals a failure to comply with any requirement set forth in this Addendum, Chargify shall promptly provide a plan to remediate the failure and begin remediation. Chargify shall bear all reasonable costs for controlled re-verification of the remediation of any such issue.

12. Return or Destruction of personal data. On expiration of the Services Agreement or any earlier termination, or on Customer's request at any time, Chargify shall return or destroy (at customer's cost if third party data migration services are required) any personal data that is within its control; provided, however, that: (i) on Customer's request, Chargify shall not destroy the personal data until it has given Customer access to the personal data for a reasonable period of time as necessary to complete an orderly migration of the personal data to Customer's or a substitute provider's systems, (ii) if Customer requires Chargify to return or destroy personal data prior to the expiration or termination of the Services Agreement, Chargify is excused from performing those Services that it is unable to perform as a result of the return or destruction, and (iii) Chargify is not required to return or destroy personal data to the extent it is expressly permitted to retain the personal data under Section 3 (Permitted Use and Disclosure) above provided that, it provides a written description of any personal data that it proposes to retain with a statement of the reasons for retention, and shall cooperate with Customer's reasonable requests to address record keeping if required. On Customer's request, Chargify shall provide a certification (signed by its executive offer) that return or destruction has been completed in accordance with this Addendum.

13. Customer Obligations. Customer makes the following representations, warranties, and covenants: (i) the personal data has been collected in accordance with applicable law, including any notices and consents legally required for Chargify to access and process the personal data in accordance with the Services Agreement, (ii) the transfer of the personal data to Chargify for the purpose of Chargify providing the Services is authorized under applicable law, (iii) Customer shall comply with applicable law as to requests from data subjects in connection with the personal data, (iv) Customer shall disclose to Chargify only that personal data that is necessary for Chargify to provide the Services in accordance with the Services Agreement, (v) Customer shall not ask Chargify to take any action with respect to the personal data the Customer is not permitted to take directly, (vi) the personal data does not include any sensitive personal data, and (vii) Customer shall indemnify and hold harmless Chargify from any and all claims, losses, or damages (including reasonable attorney fees, costs and regulatory fines) arising from Customer's breach of this Section.

14. General.

14.1 Term and Termination. This Addendum is effective as of the Effective Date and shall continue in effect for so long as Chargify continues to have access to or process personal data. This Addendum survives the expiration or termination of the Services Agreement for so long as Chargify has access to or processes personal data. If Chargify violates this Addendum, Customer may terminate this Agreement and the Services Agreement for breach. Customer may, in its sole discretion, give Chargify an opportunity to cure any violation, and may suspend Chargify's access to or processing of the personal data during the cure period.

14.2 Notices. Except as otherwise expressly stated otherwise in this Addendum, notices required under this Addendum shall be given in writing in the manner required in the Services Agreement. If Customer has provided a privacy notice contact, Chargify shall also notify Customer's privacy notice contact.

14.3 Precedence and Interpretation. This Addendum is intended to supplement the Services Agreement. If there is a conflict between this Addendum and the Services Agreement, this Addendum controls. If there is a conflict between the terms of Schedule 1 to this Addendum and the body of this Addendum, Schedule 1 controls. Any ambiguity in this Addendum as to a matter covered by applicable law should be interpreted in a way that conforms to applicable law.

14.4 Rights in Data. As between Customer and Chargify, Customer retains all right, title and interest in and to the personal data.

14.5 Assignment, Change in Control. Chargify must give Customer advance written notice of any transaction that will result in a change of control of Chargify or any sub-processor, or assignment or transfer of this Agreement or any sub-processor agreement. If Customer reasonably concludes that the following the transaction the Chargify or its successor does not have the operational or financial strength to perform the Chargify's obligations under this Agreement, Customer may terminate the Services Agreement without liability. The requirements of this Subsection are in addition to any requirements stated in the Services Agreement and apply notwithstanding anything to the contrary in the Services Agreement.

14.6 Confidential Information. Any additional or more stringent protections or remedies available with respect to information defined as “confidential information” or with like term under the Services Agreement apply to personal data.

[End]
Attach: Schedule 1(Europe and United Kingdom Specific Terms and Standard Contractual Clauses.

SCHEDULE 1

Standard Contractual Clauses for Processors

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: Ziflow Limited
Address: Alton House, 66 High Street
Northwood, Middlesex,HA6
1BL UK
Tel.: +1 (855) 494-3569
Fax: N/A
E-mail: security@ziflow.com
Other information needed to identify the organisation:
N/A

(the data exporter)

And

Name of the data importing organisation: Chargify, LLC
Address: 122 E. Houston Street Ste 105, San Antonio, Texas 78205
Tel.: 1 (800) 401-2414 (U.S.); +1 (617) 249-4603 (Intl.); e-mail: privacy@chargify.com
Other information needed to identify the organisation: n/a

(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 to Attachment 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(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 ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(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 Member State 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 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 relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(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, 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, 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 providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority 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

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 supervisory authority with regard to the processing of the data transferred;

(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 supervisory authority;

(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 supervisory authority;
(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
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 supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority 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 Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from 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. 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 law of the Member State in which the data exporter is established.

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 data exporter's data protection supervisory authority.

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 supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter

Name (written out in full): Mat Atkinson

Position: Director

Address: Alton House, 66 High Street
Northwood, Middlesex,HA6 1BL UK

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

Signature:
7/8/2021

DocuSigned by:
Mat Atkinson
9F7DADFDD26348D...

On behalf of the data importer

Name (written out in full):

Position:

Address: 122 E. Houston Street, San Antonio, Texas 78205

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

Signature:

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Export of information relating to billing and invoicing services provided by Chargify

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
Provider of online subscription billing services and related services.

Data subjects
Individuals whose subscriber and payment data are transmitted to Chargify by the Chargify customer for the purpose of using the Chargify service.

Categories of data
Names, contact information (address and telephone), e-mail address, and payment information of customer's subscribers.

Any other personal data that the Chargify customer chooses to send and store within the Chargify service.

Special categories of data (if appropriate)

The personal data transferred concern may include the following special categories of data (please specify):
None

Processing operations
The personal data transferred will be subject to one or more the following basic processing activities (please specify):
Processing as necessary to provide the Chargify services in accordance with the service agreement between Chargify and its customer.

DATA EXPORTER

Name: Mat Atkinson

Authorised Signature: DocuSigned by: Mat Atkinson 9F7DADFDD26348D...

7/8/2021

DATA IMPORTER

Name:

Authorised Signature:

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):

Data Importer shall protect the personal data from unauthorized access or acquisition, use, disclosure, loss, corruption, alteration and unavailability using those physical, technical, organizational, and administrative safeguards described below.

PCI DSS. Data Importer complies with the Payment Card Industry Data Security Standards, version 3.2.1, Level 1 ("PCI DSS"). Data Importer shall obtain an annual audit of its compliance with PCI DSS by a Qualified Security Assessor Company and, on Data Exporter's written request, shall provide its most recent PCI DSS audit report.

SOC 1. Data Importer shall implement and maintain the controls described in its Report on Controls that is part of an annual SSAE-16 SOC 1, Type 2 audit report (the "SOC 1 Report"). On Data Exporter's written request, Data Importer shall provide its most recent SOC 1 Report.

DATA EXPORTER

Name: Mat Atkinson

Authorised Signature:

7/8/2021

DocuSigned by:

Mat Atkinson

9F7DADFDD26348D...

DATA IMPORTER

Name:

Authorised Signature:

Certificate Of Completion

Envelope Id: 12777FE0B231443E939887B22DC5C440		Status: Sent
Subject: Chargify GDPR DPA & SCCs		
Source Envelope:		
Document Pages: 19	Signatures: 3	Envelope Originator:
Certificate Pages: 5	Initials: 0	Samuel Hanna V
AutoNav: Enabled		122 E Houston St
EnvelopeId Stamping: Enabled		#105
Time Zone: (UTC-06:00) Central Time (US & Canada)		San Antonio, TX 78205
		sam.hanna@chargify.com
		IP Address: 212.132.160.106

Record Tracking

Status: Original 7/8/2021 6:00:35 AM	Holder: Samuel Hanna V sam.hanna@chargify.com	Location: DocuSign

Signer Events	Signature	Timestamp
Mat Atkinson security@ziflow.com Security Level: DocuSign.email ID: 1 7/8/2021 6:00:36 AM	DocuSigned by: Mat Atkinson 9F7DADFDD26348D... Signature Adoption: Pre-selected Style Using IP Address: 212.132.160.106	Sent: 7/8/2021 6:00:36 AM Viewed: 7/8/2021 6:00:44 AM Signed: 7/8/2021 6:03:56 AM
Electronic Record and Signature Disclosure: Accepted: 7/8/2021 6:00:44 AM ID: bbc4caee-9511-4d4a-b31a-ec63364eac1a		
Samuel Hanna, V sam.hanna@chargify.com Compliance Manager Chargify Security Level: Email, Account Authentication (Optional)		Sent: 7/8/2021 6:03:57 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/8/2021 6:00:36 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Chargify (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Chargify:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: support@chargify.com

To advise Chargify of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at support@chargify.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Chargify

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to support@chargify.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Chargify

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to support@chargify.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Chargify as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Chargify during the course of your relationship with Chargify.