Data Processing Addendum

This Data Processing Addendum ("DPA") is effective as of ______, 2022 ("Effective Date"), and forms part of and is incorporated into the Chargifi SaaS Service Agreement ("Agreement") between Chargifi Limited, with its registered office at c/o Virtual Company Secretary Ltd, 7 York Road, Woking, GU22 7XH, UK (including its affiliate Chargifi Inc., a Nevada corporation, with offices at 4500 140th Avenue North, Suite 101, Clearwater, Florida, 33762, each trading as Kadence ("Chargifi" or "Company") and the Customer entity that is a party to the Agreement ("Customer"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. Unless clearly stated otherwise, references to "Sections" in this DPA refer to sections of this DPA.

1. Definitions

"Data Protection Laws" means all data protection laws and regulations applicable to a party's processing of Personal Data under the Agreement, including, where applicable, European Data Protection Law and Non-European Data Protection Laws.

"European Data Protection Law" means all data protection laws and regulations applicable to Europe, including, where applicable, Regulation 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") and any member state law implementing the same.

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"Non-European Data Protection Laws" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. ("CCPA") and the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA").

"Personal Data" means any information relating to an identified or identifiable natural person that is (i) included in Customer Data that Chargifi processes on behalf of Customer in the course of providing the Services; and (ii) subject to the Data Protection Laws.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Personal Data on systems managed or otherwise controlled by Chargifi.

"Sensitive Data" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws.

"2010 Standard Contractual Clauses" or "SCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The 2010 Standard Contractual Clauses are in Annex C hereto.

"2021 Standard Contractual Clauses" means the standard data protection clauses (processor-to-processor module) between Chargifi Limited (Ireland) and Chargifi Inc. for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021.

"Sub-processor" means any processor engaged by Chargifi to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA, as described in Article 28 of the GDPR. Sub-processors may include third parties but shall exclude Chargifi employees, contractors, or consultants.

The terms "controller", "data subject", "processor" and "processing" shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and "process," "processes" and "processed", with respect to any Personal Data, shall be interpreted accordingly.

2. Roles and Responsibilities

2.1 Parties' roles. If European Data Protection Law applies to either party's processing of Personal Data, the parties acknowledge and agree that with regard to the processing of Personal Data, Customer is the controller and Chargifi is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA. For the avoidance of doubt, this DPA shall not apply to instances where Chargifi is the controller (as defined by European Data Protection Law) unless otherwise described in Annex D hereto.

2.2 Purpose limitation. Chargifi shall process Personal Data only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing. The parties agree that the Agreement sets out Customer's complete instructions to Chargifi in relation to the processing of Personal Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 Prohibited data. Customer will not provide (or cause to be provided) any Sensitive Data to Chargifi for processing under the Agreement, and Chargifi will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Sensitive Data.

2.4 Customer compliance. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Personal Data and any processing instructions it issues to Chargifi; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Chargifi to process Personal Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to the collection of employee personal data or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.

2.5 Lawfulness of Customer's instructions. Customer will ensure that Chargifi's processing of the Personal Data in accordance with Customer's instructions will not cause Chargifi to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Chargifi shall promptly notify Customer in writing, unless prohibited from doing so under European Data Protection Laws, if it becomes aware or believes that any data processing instruction from Customer violates Data Protection Laws.

3. Sub-processing

3.1 Authorized Sub-processors. Customer hereby authorizes Chargifi to engage Sub-processors to Process Personal Data on Customer's behalf, including the Sub-processors currently engaged by Company and listed in Annex A to this DPA. Customer agrees that Chargifi may engage Sub-processors to process Personal Data on Customer's behalf. Chargifi shall notify Customer if it adds or removes Sub-processors at least 10 days prior to any such changes, which may be done by email or posting on a website identified by Chargifi to Customer.

3.2 Sub-processor obligations. Chargifi shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the service provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Chargifi to breach any of its obligations under this DPA.

4. Security

4.1 Security Measures. Chargifi shall implement and maintain appropriate technical and organizational security measures that are designed to protect Personal Data from Security Incidents and designed to preserve the security and confidentiality of Personal Data in accordance with Chargifi's security standards described in Annex B hereto ("Security Measures").

4.2 Confidentiality of processing. Chargifi shall ensure that any person who is authorized by Chargifi to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Updates to Security Measures. Customer is responsible for reviewing the information made available by Chargifi relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Chargifi may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

4.4 Security Incident response. Upon becoming aware of a Security Incident, Chargifi shall: (i) notify Customer without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Chargifi's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Chargifi of any fault or liability with respect to the Security Incident.

4.5 Customer responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Personal Data when in transit to and from the Services, and taking any appropriate steps to securely encrypt or backup any Personal Data uploaded to the Services.

5. Audits. Chargifi shall provide written responses (on a confidential basis) to all commercially reasonable requests for information made by Customer regarding Processing of Personal Data, including responses to information security reviews, that are necessary to confirm Chargifi's compliance with this DPA. To the extent Chargifi's responses are not sufficient to enable customer to satisfy its obligations under applicable Data Protection Laws, Chargifi shall cooperate with audits and inspections performed by Customer or a vendor of Customer reasonably acceptable to Chargifi, provided however, that any audit or inspection: (i) may not be performed unless necessary to determine Chargifi's compliance with this DPA and Customer reasonably believes that Chargifi is not complying with this DPA, or as otherwise specifically required by applicable Data Protection Laws; (ii) must be conducted at Customer's sole expense and subject to reasonable fees and costs charged by Chargifi; (iii) may be conducted on no less than thirty (30) days prior written notice from Customer, at a date and time and for a duration mutually agreed by the parties; and (iv) must be performed in a manner that does not cause any damage, injury, or disruption to Chargifi's premises, equipment, personnel, or business. Notwithstanding the foregoing, Chargifi will not be required to disclose any proprietary or privileged information to Customer or an agent or vendor of Customer in connection with any audit or inspection undertaken pursuant to this DPA.

6. Data Transfers and Location

6.1 Transfers. Personal Data that Chargifi processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with this DPA and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Chargifi to transfer Personal Data to the United States or any other country in which Chargifi or its Sub-processors operate and to store and process Personal Data to provide the Services, except as described elsewhere in this DPA.

6.2 Standard Contractual Clauses. All transfers of Personal Data originating in the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Services to a country that is not recognized as providing an adequate level of protection for Personal Data shall be governed by the 2021 Standard Contractual Clauses implemented by Chargifi. In addition, such transfers from the United Kingdom and Switzerland shall be governed by the 2010 Standard Contractual Clauses. For the purposes of the descriptions in the 2010 Standard Contractual Clauses, Chargifi agrees that it is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be an entity located outside Europe), as further described on the attached Annex A.

6.3 Inconsistency. In the case of any inconsistency between the 2021 Standard Contractual Clauses and the 2010 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Personal Data under applicable law.

6.4 Alternative transfer mechanism. To the extent Chargifi adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield) for the transfer of European Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Law and extends to the countries to which European Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer European Data (within the meaning of applicable European Data Protection Law), Chargifi may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of European Data.

7. **Return or Deletion of Data**. Upon termination or expiration of the Agreement, Chargifi shall (at Customer's election) delete or return to Customer all Personal Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Chargifi is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data Chargifi shall securely isolate, protect from any further processing and eventually delete in accordance with Chargifi's deletion policies, except to the extent required by applicable law.

8. **Data Subject Rights and Cooperation**

8.1 Data subject requests. Chargifi shall, taking into account the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made to Chargifi directly, Chargifi shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If Chargifi is required to respond to such a request, Chargifi shall promptly notify Customer and provide Customer with a copy of the request unless Chargifi is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Chargifi from responding to any data subject or data protection authority requests in relation to Personal Data for which Chargifi is a controller.

8.2 Data protection impact assessment. To the extent required under applicable Data Protection Laws, Chargifi shall (taking into account the nature of the processing and the information available to Chargifi) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Chargifi shall comply with the foregoing by: (i) complying with Section 5 (Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. **Jurisdiction-Specific Terms**. To the extent Chargifi processes Personal Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex D, then the terms specified in the attached Annex D with respect to the applicable jurisdiction(s) (“Jurisdiction-Specific Terms”) apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms’ applicability to Chargifi.

10. **Limitation of Liability**

10.1 Each party's and its affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against Chargifi or its affiliates under or in connection with this DPA (including, where applicable, the Standard Contractual Clauses) shall be brought solely by Customer.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. **Relationship with the Agreement**

11.1 This DPA shall remain in effect for as long as Chargifi carries out Personal Data processing operations on behalf of Customer or until termination of the Agreement (and all Personal Data has been returned or deleted in accordance with Section 7 above).

11.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Services.

11.3 In the event of any conflict or inconsistency between this DPA and the Chargifi SaaS Service Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) Standard Contractual Clauses; then (ii) this DPA; and then (iii) the Chargifi SaaS Service Agreement.

11.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

11.6 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

By signing below, the Parties agree to be bound by the terms and conditions of this DPA, effective as of the Effective Date stated above. This DPA may be executed in one or more counterparts.

CHARGIFI	**CUSTOMER**
By: ______________________________	By: ______________________________
Name: ____________________________	Name: ____________________________
Title: _____________________________	Title: _____________________________

Annex A – Details of Data Processing

(a) Controller (data exporter): Customer

(b) Processor (data importer): Chargifi Inc.

(c) Subject matter: The subject matter of the Processing is Chargifi's provision to Customer of the Services.

(d) Duration of processing: Chargifi Inc. will process Personal Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(e) Nature and Purpose of processing: Chargifi Inc. will process Personal Data for the Permitted Purposes, including for the purposes of: (a) setting up, operating, monitoring, and providing the Service; (b) communicating with users of the Service; and (c) executing other agreed-upon written instructions of Customer.

(f) Nature of the processing: Chargifi provides a meeting scheduling service, and other related services, as more particularly described in the Agreement.

(g) Categories of data subjects:
The Categories of Data Subjects may include the following:

- employees and contractors of Customer; and
- current and prospective customers and business partners of Customer who are natural persons.

(h) Types of Personal Data: Customer may upload, submit or otherwise provide certain personal data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and may include the following types of Personal Data:

- Users Identification and contact data (name, email, job title, contact details, city of residence, profile photograph, work schedule, biography); space reservation (reservation time, check-out time, space identifier, meeting details, self-certification data);
- images, content, and messages shared by and between Customer employees and contractors through the Service; and
- such other Personal Data as may be submitted by Customer as reasonably necessary for Customer to receive or use the Service.

(i) Sensitive Data: Chargifi does not want to, nor does it intentionally, collect or process any Sensitive Data in connection with the provision of the Service. Special categories of data are not required to use the Service. Customer and its users may submit special categories of data to the Services, the extent of which is determined and controlled by Customer and attendees in their sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning an individual's health or sex life.

(j) Sub-processors:

Direct Sub-Processors	Purpose
Work OS	Automated User provisioning tool – may contain Customer Contact Details
Google	Calendar tools utilised when google integration is enabled
Microsoft	Calendar tools utilised when google integration is enabled
Indirect Sub-Processors	Purpose
Xero	Accounting System – Contains billing contact names and email addresses.
HubSpot	Customer Relationship Management System – Contains Sales and Marketing contact names, addresses and contact details
Panda Doc	Customer Quote and Pricing System - Contains Sales and Marketing contact names, addresses and contact details

Zendesk	Customer Ticketing System – Contains Customer Contact information
Google	Administration and Filing System – Contains administrative data including and customer contact and contractual information.
Expensify	Expenses Management System – may contain some Customer Name information where expenses have been incurred for Client Entertainment.
Docusign	Document Management and Signing System – may contain Customer Contact Information where a non-standard contract has been used.
Slack	Communication System – May contain Customer names and addresses.
Zoom	Communication System – May contain recordings that note Customer names and addresses
Mailchimp	Email Marketing Platform – Will contain Customer Contact Details
Sub-Contractors	Purpose
Amazon Web Services	Data Hosting and Infrastructure Platform.

Annex B – Security Measures

The Security Measures applicable to the Service are described below.

- Chargifi uses Data Centres based in the Republic of Ireland.
- Chargifi Wx Cloud is hosted by Amazon Web Services (AWS) and provides a strong level of security in retaining our data. For more information about secure data storage, please refer to AWS security and AWS Certifications

Protection from Data Loss, Corruption

- Our multi-tenancy solution achieves data isolation with the use of row-base separation. We have strict controls (policy, procedure and coding standards) in place to eliminate the risk of Personal Data being exposed beyond its own tenant.
- Personal Data is stored in multiple availability zones and regularly backed up.

Application Level Security

- All passwords are salted and hashed using a one-way encryption algorithm for further protection. It is not possible to recover a stored password, these can only be reset through our “Forgotten Password” process.
- All login pages (from our website and mobile website) pass data via HTTPS/TLS 1.2+.
- The entire Chargifi application is encrypted with HTTPS/TLS 1.2+.
- Our systems are penetration-tested annually by independent third-party specialists. Any vulnerabilities discovered are tracked and addressed as a matter of urgency.
- Our mobile applications are tested to the OWASP MASVS standard.

Internal IT Security

- Chargifi Offices are secured by keycard access and biometrics, and they are monitored with cameras throughout.

Internal Protocol and Education

- We continuously train employees on best security practices, including how to identify social engineering, phishing scams, and hackers.
- All employees sign a Privacy Agreements an part of their employment contracts and our Human Resources Policies make it clear that a Data Privacy Breach can be treated as a matter of Gross Misconduct.

In order to protect our company from a variety of different losses, Chargifi has established an insurance program. which includes [coverage for cyber incidents, error and omissions, property and business interruption coverage, as well as international commercial general liability coverage].

Security Reporting

If you’ve discovered a vulnerability in the Chargifi application, please report it to us at the email address noted below. Chargifi strives to stay on top of the latest security developments both internally and by working with third parties. We appreciate the community’s efforts in creating a more secure web.

If you believe your account has been compromised or you are seeing suspicious activity on your account please report it immediately to info-security@chargifi.com.

Annex C – 2010 Standard Contractual Clauses

Standard Contractual Clauses
2010 Standard contractual clauses for the transfer of personal data from the Controller to third countries (controller to processor transfers)

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, Chargifi Inc., a Nevada corporation, with offices at 4500 140th Avenue North, Suite 101, Clearwater, Florida, 33762 (hereinafter the "data importer") and Customer (hereinafter the "data exporter") 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 Annex 1.

Clause 1
Definitions
For the purposes of the Clauses:

- '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;
- 'the data exporter' means the controller who transfers the personal data;
- '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;
- '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;
- 'the 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;
- '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:

- 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 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;
- 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 Data Protection Law and the Clauses;
- that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- that after assessment of the requirements of the 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;
- that it will ensure compliance with the security measures; 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;
- 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;
- 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;
- 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
- that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- 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;
- 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;
- that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- that it will promptly notify the data exporter about:

  - 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,
  - any accidental or unauthorised access, and
  - any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- 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;
- 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;
- 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;
- that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- 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:
   - to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   - 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 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 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.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES
Details of the transfer:
Please see the details set forth in Annex A to the Data Processing Addendum ("DPA") to which these Clauses are appended.
APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES
Please see Annex B for a 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).

Signing the Standard Contractual Clauses, Appendix 1, and Appendix 2 on behalf of the data importer:

CHARGIFI INC.

By: ______________________________

Name: ____________________________

Title: _____________________________

Annex D - Jurisdiction-Specific Terms

Europe:

1. Objection to Sub-processors. Customer may object in writing to Chargifi's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of the DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Chargifi will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).
2. Government data access requests. As a matter of general practice, Chargifi does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Chargifi accounts (including Personal Data). If Chargifi receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a Chargifi account (including Personal Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Chargifi shall: (i) inform the government agency that Chargifi is a processor of the data; (ii) attempt to redirect the agency to request the data directly from Customer; and (iii) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy. As part of this effort, Chargifi may provide Customer's primary and billing contact information to the agency. Chargifi shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or Chargifi's property, the Chargifi site, or Services.

California:

1. Except as described otherwise, the definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA.
2. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Personal Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.
3. Chargifi's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer's rights under the CCPA.
4. Chargifi may de-identify or aggregate Personal Data as part of performing the Services specified in this DPA and the Agreement. Notwithstanding anything to the contrary herein, Chargifi shall have the right to collect and analyze data and other information relating to the provision, use and performance of various aspects of the Services and related systems and technologies (including, without limitation, information concerning Personal Data and other information produced by Customer through the Services, and data and insights derived therefrom) on an aggregated and anonymized basis, and Chargifi will be free (during and after the term hereof) to (i) use such information and data internally to improve and enhance the Services and for other development, diagnostic and corrective purposes in connection with the Services and other Chargifi offerings, and (ii) disclose such data solely in aggregate and de-identified form in connection with its business. No rights or licenses are granted except as expressly set forth herein.