Data Processing Addendum

This Data Processing Addendum ("DPA") forms part, amends, and supplements the Order Form and Terms and Conditions (together, the "Agreement") between the Chargifi entity that is a party to the Agreement ("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, UK 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

"European Restricted Transfer" means a transfer (or onward transfer) to a Third Country of Personal Data originating in Europe for which European Data Protection Law requires the establishment of appropriate safeguards.

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

"Non-European Data Protection Laws" means (i) U.S. state privacy laws, including without limitation the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. ("CCPA"), the Virginia Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 et seq., the Colorado Privacy Act, Colorado Revised Statute Title 6 Article 1 Part 13 § 6-1-1301 et seq., the Connecticut Data Privacy Act, Connecticut Public Act No. 22-15, and the Utah Consumer Privacy Act,
Utah Code Annotated Title 13 Section 2 § 1 et seq., and (ii) 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 Company 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 Company.

"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.

"2021 Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as approved by the European Commission in Commission Implementing Decision (EU) 2021/914, dated 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

"Sub-processor" means any processor engaged by Company 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 Company employees, contractors, or consultants.

"Third Country" means any country, organization, or territory not acknowledged by the European Commission or the UK government, as applicable, to ensure an adequate level of protection for Personal Data in accordance with GDPR or UK Data Protection Law, as applicable.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018 and in force as of 21 March 2022, as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, and as revised by the UK Information Commissioner's Office from time to time.

"UK Data Protection Law" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the United Kingdom, including the UK GDPR and the Data Protection Act 2018.

"UK Restricted Transfer" means a transfer (or onward transfer) to a Third Country of Personal Data originating in the United Kingdom for which UK Data Protection Law requires the establishment of appropriate safeguards.

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. With regard to the processing of Personal Data, Customer is the controller and Company is a processor acting on behalf of Customer, as further described in Annex A (Details of Data Processing) of this DPA.

2.2 Purpose limitation. Company 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 and this DPA set out Customer's complete instructions to Company 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 Company for processing under the Agreement, and Company 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 Company; 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 Company 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 Company's processing of the Personal Data in accordance with Customer's instructions will not cause Company to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Company 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 Company 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. Company shall notify Customer if it adds a new Sub-processor at least 10 days prior to any such change, which may be done by email or posting on a website identified by Company to Customer. Customer may object in writing to Company's appointment of a new Sub-processor within five (5) calendar days of receiving notice from Company, 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, Company 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).

3.2 Sub-processor obligations. Company 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 Company to breach any of its obligations under this DPA.

4. Security

4.1 Security Measures. Company 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 Company's security standards described in Annex B hereto ("Security Measures").

4.2 Confidentiality of processing. Company shall ensure that any person who is authorized by Company 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 Company 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 Company 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, Company 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. Company's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Company 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. Company 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 Company's compliance with this DPA. To the extent Company's responses are not sufficient to enable customer to satisfy its obligations under applicable Data Protection Laws, Company shall cooperate with audits and

inspections performed by Customer or a vendor of Customer reasonably acceptable to Company, provided however, that any audit or inspection: (i) may not be performed unless necessary to determine Company's compliance with this DPA and Customer reasonably believes that Company 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 Company; (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 Company's premises, equipment, personnel, or business. Notwithstanding the foregoing, Company 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. Processing Locations; Restricted Transfers

6.1 Authorization for International Transfers. Subject to the terms of this Section, Customer authorizes Company to transfer Personal Data to the United States or any other country in which Company or its Sub-processors operate or maintain facilities and to store and process Personal Data in such locations as necessary to provide the Services. Company will ensure, and will be responsible for ensuring, that any such transfers comply with the requirements of applicable Data Protection Laws, including, where the transfer involves a European Restricted Transfer or UK Restricted Transfer, by implementing appropriate safeguards for the transfer such as by entering into the 2021 Standard Contractual Clauses or UK Addendum with the relevant data importer.

6.2 European Restricted Transfers. If and to the extent Company's performance or Customer's use of the Services involve a European Restricted Transfer in which Customer acts as the data exporter and Company acts as the data importer, and no Alternative Transfer Mechanism (as defined in Section 6.4) applies, the 2021 Standard Contractual Clauses, which are incorporated by reference herein, will apply to such European Restricted Transfer, as supplemented by the points below:

(a) Where the 2021 Standard Contractual Clauses require the parties to select a module, the parties select Module Two (Transfer Controller to Processor).

(b) Clause 7 of the 2021 Standard Contractual Clauses, the "Docking Clause – Optional," shall be deemed incorporated.

(c) In clause 9 of the 2021 Standard Contractual Clauses, the Parties select Option 2 (General Written Authorization), which shall be enforced in accordance with Section 3 (Sub-Processing) of this DPA.

(d) The optional wording in clause 11 of the 2021 Standard Contractual Clauses shall not be deemed incorporated.

(e) In clause 17 of the Clauses, the Parties agree that the 2021 Standard Contractual Clauses shall be governed by the laws of Ireland.

(f) In clause 18 of the 2021 Standard Contractual Clauses, the Parties agree that any dispute arising from the Clauses shall be resolved by the courts of Ireland.

(g) Annex I.A, I.B and I.C of the 2021 Standard Contractual Clauses shall be deemed completed with the information set out in Annex A to this DPA. Annex II of the 2021 Standard Contractual Clauses shall be deemed completed with the information set out in Annex B to this DPA.

(h) If and to the extent the transfer involves Personal Data originating from Switzerland and is subject to the Swiss Federal Act on Data Protection of 19 June 1992 (the "FADP"), the 2021 Standard Contractual Clauses are deemed to be supplemented with an additional annex that provides as follows:

i. for purposes of Clause 13 and Annex I.C, the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner;

ii. the term “member state” as used in the 2021 Standard Contractual Clauses must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with clause 18.c; and

iii. references in the 2021 Standard Contractual Clauses to the GDPR should be understood as references to the FADP.

(i) Nothing in this DPA or in the Agreement is intended by the Parties to be construed as prevailing over the 2021 Standard Contractual Clauses.

6.3 UK Restricted Transfers. If and to the extent Company’s performance of the Services involves a UK Restricted Transfer in which Customer acts as the data exporter and Company acts as the data importer and no Alternative Transfer Mechanism, as defined in Section 6.4, applies, the UK Addendum, which is incorporated by reference herein, will apply to such UK Restricted Transfer, as supplemented by the points below:

(a) Table 1 is deemed to be completed with the parties’ details and contact information as set forth in Annex A.

(b) For the purposes of Table 2, the Addendum EU SCCs are the 2021 Standard Contractual Clauses entered into between Customer and Company under Section 6.2 of this DPA.

(c) For the purposes of Table 3, the Appendix Information is set forth in Annex A and Annex B to this DPA.

(d) In Table 4, the parties select both “Importer” and “Exporter.”

(e) Nothing in this DPA or in the Agreement is intended by the Parties to be construed as prevailing over the UK Addendum.

6.4 Alternative transfer mechanism. To the extent Company adopts an alternative data export mechanism (including any new version of or successor to the EU-US Privacy Shield) for European Restricted Transfers or UK Restricted Transfers not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA upon written notice from Company to Customer (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Law or UK Data Protection Law, as applicable, and applies to the relevant European Restricted Transfer or UK Restricted Transfer). 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 Personal Data as part of a European Restricted Transfer or UK Restricted Transfer, Company 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, Company 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 Company 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 Company shall securely isolate, protect from any further processing and eventually delete in accordance with Company's deletion policies, except to the extent required by applicable law.

8. Data Subject Rights and Cooperation

8.1 Data subject requests. Company shall, taking into account the nature of the processing, provide reasonable 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 Company directly, Company 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 Company is required to respond to such a request, Company shall promptly notify Customer and provide Customer with a copy of the request unless

Company is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Company from responding to any data subject or data protection authority requests in relation to Personal Data for which Company is a controller.

8.2 Data protection impact assessment. To the extent required under applicable Data Protection Laws, Company shall (taking into account the nature of the processing and the information available to Company) 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. Company 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 Company processes Personal Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex C, then the terms specified in the attached Annex C 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 Company.

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 Company or its affiliates under or in connection with this DPA (including, where applicable, the 2021 Standard Contractual Clauses or UK Addendum) 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 Company 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 Agreement, the provisions of the following documents (in order of precedence) shall prevail: (i) the UK Addendum or 2021 Standard Contractual Clauses, when applicable; then (ii) this DPA; and then (iii) the 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.

Annex A – Details of Data Processing

A. LIST OF PARTIES

Data exporter(s):
Name: The entity identified as "Customer" in the Agreement.
Address: The address for Customer as specified in the Agreement or as otherwise provided to Company.
Contact person's name, position and contact details: The contact details for Customer as specified in the Agreement.
Activities relevant to the data transferred under these Clauses: Customer's use of the Services pursuant to the Agreement and the DPA.
Signature and date: By entering into the Agreement, Customer will be deemed to have signed this Annex A.
Role (controller/processor): Controller.

Data importer(s):
Name: The Chargifi contracting party as set forth in the Agreement.
Address: The address for the Chargifi contracting party as set forth in the Agreement.
Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses: Provision of the Services to Customer pursuant to the Agreement and the DPA.
Signature and date: By entering into the Agreement, Company will be deemed to have signed this Annex A.
Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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.

Categories of personal data transferred

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.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not Applicable—Customer is prohibited from using the Services to Process Sensitive Data.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal Data may be transferred on a continuous basis during the Term of the Agreement.

Nature of the processing

The nature of the processing is Company's provision of the Services under the Agreement, including meeting scheduling and other related services, including for the purposes of (a) setting up, operating, monitoring, and providing the Services; (b) communicating with Users; and (c) executing other agreed-upon written instructions of Customer.

Purpose(s) of the data transfer and further processing
The purpose of the data transfer and further processing is Company's provision of the Services under the Agreement to enable Customer's and its' users use of Company's meeting scheduling and other related services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained for the duration of the Agreement and subject to the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors will Process Personal Data as necessary to perform the Service pursuant to the Agreement. Subject to the DPA, Sub-processors will Process Personal Data for the duration of the Agreement.

As of the date of the Agreement, the Sub-Processors engaged by Chargifi are listed at https://kadence.co/sub-processors/

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

For the purposes of the 2021 Standard Contractual Clauses, the competent supervisory authority will be the supervisory authority that has supervision over Customer. If Customer is not based in the EEA but is subject to the GDPR, the competent supervisory authority will be the Irish Data Protection Commission.

Annex B – Security Measures

The Security Measures applicable to the Service are described below.

- Company uses Data Centres based in the Republic of Ireland.
- The Kadence Platform 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 (https://aws.amazon.com/security/) and AWS Certifications (https://aws.amazon.com/compliance/)

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 Kadence Platform 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

- Company 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 as 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.

Annex C - Jurisdiction-Specific Terms

Europe and the United Kingdom

Government data access requests. As a matter of general practice, Company does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Company accounts (including Personal Data). If Company 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 Company account (including Personal Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Company shall: (i) inform the government agency that Company 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, Company may provide Customer's primary and billing contact information to the agency. Company shall not be required to comply with this section 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 Company's property, the Company site, or Services.

California:

CCPA. To the extent that Personal Data processed by Company on Customer's behalf includes "Personal Information" as that term is defined under the CCPA, the following terms will apply to Company's processing of such CCPA-covered Personal Information in addition to the terms of the DPA.

(a) Company will not (i) "sell" or "share" (as those terms are defined in the CCPA) Personal Information; (ii) retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing functions under the Agreement and under this DPA, including retaining, using, or disclosing Personal Information for a commercial purpose other than performing the Services and for the specific purposes described in Annex A; (iii) retain, use, or disclose Personal Information outside of the direct business relationship between Company and Customer; or combine Personal Information received in connection with performing functions under the Agreement and under this DPA with Personal Information it receives from another source except to perform Business Purposes (as defined by and specified in the CCPA).

(b) Notwithstanding the foregoing, Customer agrees that Company may, if otherwise permitted by CCPA and subject to Company's confidentiality obligations hereunder, process Personal Information to the extent permitted or required by applicable law, including to perform other processing functions permitted for "Service Providers" under the CCPA.

(c) In connection with providing the Services, Company will also: (i) comply with the CCPA and provide the same level of privacy protection as is required by the CCPA for Personal Information; (ii) allow Customer to take reasonable and appropriate steps to help ensure that Company uses Personal Information in a manner consistent with Customer's obligations under the CCPA; (iii) notify Customer promptly in writing if it makes a determination that it can no longer meet its obligations under the CCPA; and (iv) permit Customer to, upon notice, take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information. Company understands the restrictions set forth in this Section and will comply with them.