Data Protection Agreement

This Data Protection Agreement (the "DPA") is executed as of the Effective Date of the Agreement as defined below (the "DPA Effective Date") between OneBill Software, Inc. ("COMPANY") and its customer named in the applicable Platform Services Agreement, Order Form and or Fee Schedule signed by the parties ("Customer"). Capitalized terms have the meanings provided in the Agreement defined below except as provided here.

WHEREAS, COMPANY and Customer have executed a Platform Services Agreement or other agreement ("Agreement") governing Customer's license of, or right to access and use, the COMPANY Software and Services ("Services"); and

WHEREAS, COMPANY and Customer wish to enter this DPA, which will supplement certain provisions of the Agreement regarding each party's respective security and data protection obligations; and

WHEREAS, this DPA is not a standalone agreement and is only effective if COMPANY and Customer have previously executed an Agreement; and

NOW THEREFORE, the parties agree as follows:

1 Definitions.

a. "Data Controller" means the entity that determines the purposes and means of processing Personal Data.

b. "Data Processor" means the entity that processes Personal Data on behalf of the Data Controller, subject to the Controller's instructions.

c. "Customer" refers to the entity that engages COMPANY to process Personal Data and acts as the Data Controller.

d. "COMPANY" acts solely as a Data Processor and does not determine the purposes or means of processing Personal Data.

e. "Personal Data Breach" means a breach by COMPANY of its security obligations in this DPA that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data stored or otherwise processed in Customer's COMPANY instance as part of the Services that compromises the confidentiality, integrity, or availability of such Personal Data.

f. "Data Protection Law" means all applicable legislation relating to data protection and

privacy together with any national implementing laws in any member state of the European Union or, to the extent applicable, in any other country, state, or province, as amended, repealed, consolidated or replaced from time to time including the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") and the GDPR as transposed into United Kingdom ("UK") national law by operation of Section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR").

g. "Personal Data" means any information relating to an identified natural person or a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, in each case that is processed by COMPANY under the Agreement (each such person a "Data Subject") where such data are contained within Customer Data.

h. "Business", "Service Provider", "Process", "Processor", "Controller" and "Supervisory Authority" will each have the meaning given to them in applicable Data Protection Law.

i. "Standard Contractual Clauses" means the standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which shall automatically apply.

j. "UK Addendum" means UK Information Commissioner's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0 in force 21 March 2022.

2 Processing of Personal Data.

a. COMPANY's Role as a Data Processor
   i. Processor Only: OneBill does not collect or determine the purposes and means of processing Personal Data. All data processing activities are conducted on behalf of the Customer (the Data Controller) in accordance with their instructions.
   ii. No Independent Data Processing: OneBill does not use, sell, or share Personal Data for its own purposes. Any processing outside the scope of the Customer's instructions will require explicit written consent.
   iii. No Data Collection: The Customer is solely responsible for collecting Personal Data, obtaining necessary legal consents, and ensuring compliance with Data Protection Laws.

b. Applicability. This DPA will apply only to the extent that the Services are engaged in the processing of Personal Data subject to Data Protection Laws on behalf of Customer.

c. Relationship of the Parties. If applicable Data Protection Law recognizes the roles of Controller/Business and Processor/Service Provider as applied to Personal Data, then as between COMPANY and Customer, Customer acts as Controller and Business and COMPANY acts as a Processor/Service Provider (or Subprocessor, as the case may be) of Personal Data. Customer appoints COMPANY as a Processor to Process Personal Data: (a) for the purposes described in the Agreement, or (b) with Customer's prior written consent (collectively the "Permitted Purpose"), unless Processing is required by applicable Data Protection Law to which COMPANY is subject, in which case COMPANY shall, to the extent permitted by applicable law, inform Customer of that legal requirement before so Processing that Personal Data. Each party will comply with the obligations that apply to it under Data Protection Law in the Processing of Personal Data. If COMPANY becomes aware that Processing for the Permitted Purpose infringes Data Protection Law, it will promptly inform Customer, provided, however, COMPANY is not responsible for performing legal research and/or for providing legal advice to Customer. The details of the transfer are specified in the attached Exhibit A and incorporated herein by this reference.

d. Customer's Instructions. Any additional or different instructions from Customer pertaining to the Processing of Personal Data require a signed agreement between COMPANY and Customer and may be subject to additional fees. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. If COMPANY cannot Process Personal Data according to Customer's instructions due to a legal requirement under any applicable Data Protection Law, COMPANY will (i) promptly notify Customer of such inability, providing a reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law; and (ii) Process (or continue to process) Personal Data to the extent COMPANY is able to comply with Customer's instructions in order to provide the Services as set forth in the Agreement.

e. Customer Notices and Consents. Customer shall (a) provide all required notices and appropriate disclosures to all Data Subjects regarding Customer's, and COMPANY's, Processing of Personal Data and (b) ensure that Customer has obtained (or will obtain) and maintain during the term of the Agreement all rights and consents (if required) which are necessary for COMPANY to Process Customer Personal Data in accordance with this DPA and the Agreement. If Customer is not required by Data Protection Law to obtain and maintain valid consent from Data Subjects, Customer will otherwise comply with requirements under Data Protection Law to obtain and maintain a valid legal basis to Process Personal Data and for providing such data to COMPANY for Processing under the Agreement.

f. Confidentiality of Processing. COMPANY will treat Personal Data as Customer's Confidential Information. COMPANY shall implement processes designed to ensure that Personal Data is only made available to those of its personnel, including its Subprocessors, who (i) need to access such Personal Data in order to carry out their roles in the performance of COMPANY's obligations under the Agreement and this DPA and (ii) have committed themselves to protect the confidentiality of such

Personal Data or are otherwise under an appropriate statutory obligation of confidentiality.

g. Cooperation and Data Subjects' Rights. COMPANY will provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (a) any request from a Data Subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a Data Subject, Supervisory Authority or other third party in connection with the Processing of the Personal Data. If any such request, correspondence, enquiry or complaint is made directly to COMPANY, COMPANY will promptly inform Customer providing full details of the same to the extent Customer is identified as the relevant entity that collected the Data Subject's Personal Data and to the extent legally permitted. If a Data Subject does not identify an entity that collected its Personal Data, COMPANY will instruct the Data Subject to identify and contact the relevant entity that collected its Personal Data. COMPANY shall comply with Customer's instructions regarding the handling of a Data Subject inquiry, subject to the terms of Sections 2a. and 2b.

h. Personal Data Return and Disposal. Within 30 days after a written request by Customer or the termination or expiration of the Agreement, COMPANY will: (a) if requested by Customer, provide Customer with a copy of any Personal Data in COMPANY's possession that Customer does not already have; and (b) make reasonable efforts to securely destroy all Personal Data in COMPANY's possession in a manner that makes such Personal Data non-readable and non-retrievable. Notwithstanding the foregoing, COMPANY may retain copies of Personal Data: (x) to the extent COMPANY has a separate legal right or obligation to retain some or all of the Personal Data; (y) in its capacity as a Controller for COMPANY's business operations (such as in email records, customer support or accounting records), and (z) in backup or archive systems until such records have been overwritten or expunged in accordance with COMPANY's data retention policy.

i. California Consumer Privacy Act of 2018 ("CCPA") as amended by California Privacy Rights Act of 2020 ("CPRA"). COMPANY confirms that it understands the restrictions set forth in 1798.140(ag)(1) of the CPRA and will comply with the same to the extent the Personal Data are subject to the CPRA and no other CPRA exemptions apply.

j. Special or Sensitive Data. Unless set forth in a statement of work, order, or other document, Personal Data may not include any sensitive or special categories of data that impose specific data security or data protection obligations on COMPANY in addition to or different from those specified in any documentation or which are not provided as part of the Services. COMPANY does not require and does not request any sensitive or special categories of data to provide the Services. Customer understands and agrees that COMPANY does not differentiate between different types of data sensitivity when Processing Personal Data or treat certain types of Personal Data differently from other types and applies the same security measures to all Personal Data as set forth in this DPA.

3 **International Transfers.**

a. COMPANY will not transfer Personal Data outside the European Economic Area ("EEA") unless it takes such measures as are necessary to provide adequate protection for such Personal Data consistent with the requirements of Data Protection Law. To the extent COMPANY Processes (or causes to be Processed) any Personal Data originating from the EEA in a country that has not been designated by the European Commission or other relevant authority as providing an adequate level of protection for Personal Data, Customer and COMPANY agree that the transfer will be subject to the Standard Contractual Clauses and UK Addendum, as applicable, where Exhibit A provides the necessary information for the Appendix of the Standard Contractual Clauses and UK Addendum, or if the Standard Contractual Clauses or UK Addendum are no longer available or valid, another mechanism compliant with Data Protection Law.

4 **Subprocessing.**

a. Customer authorizes COMPANY to engage COMPANY affiliates and third party suppliers and vendors to process Personal Data for the Permitted Purpose ("Subprocessors") provided that: (a) COMPANY will maintain an up-to-date list of Subprocessors located at Annex III, which it will update with details of any change in Subprocessors; and (b) COMPANY will enter into a binding written agreement with the Subprocessor that imposes on the Subprocessor substantially the same level of restrictions that apply to COMPANY under this DPA to the extent applicable to the nature of the services provided by such Subprocessor. For the avoidance of doubt, the above authorization constitutes Customer's prior written consent to the subprocessing of Personal Data for purposes of Clause 9, Option 2 of the Standard Contractual Clauses.

b. Customers may object to COMPANY's appointment or replacement of a Subprocessor prior to its appointment or replacement, provided such objection is based on reasonable and objective grounds that the Subprocessor does not or cannot comply with applicable Data Protection Law. Customer has fifteen (15) days after COMPANY notifies customer of such new Subprocessor to notify COMPANY in writing of its objection supported by documentary evidence. Upon receipt of Customer's written objection, Customer and COMPANY will work together without unreasonable delay to find a mutually acceptable resolution to address the objection, including but not limited to reviewing additional documentation supporting the Subprocessor's ability to comply with Data Protection Law. To the extent Customer and COMPANY do not reach a mutually acceptable resolution within a reasonable timeframe, COMPANY will use reasonable endeavors to make available to Customer a change in the Services or will recommend a commercially reasonable change to the Services to prevent the applicable Subprocessor from processing Personal Data. If COMPANY is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may, as its sole remedy, suspend or terminate the Agreement in accordance with the termination provisions in the Agreement without liability to COMPANY. Customers will not receive a refund of any unused prepaid fees on such termination and if fees remain unpaid for a subscription term, Customer will

immediately pay the remaining balance due for the remainder of the subscription term.

c. Where any of its Subprocessors fails to fulfil its data protection obligations in relation to the Services provided to Customer, such that COMPANY would be found to have violated its obligations to Customer under this DPA, COMPANY will be responsible to Customer for the performance of its Subprocessor's obligations.

5 COMPANY Security Measures.

a. Security in COMPANY-Managed Deployments. In deployments where COMPANY manages the Services, COMPANY shall implement procedural, technical, and administrative safeguards designed to protect Personal Data from a Personal Data Breach when cached in the Services or in transit between Customer's databases and the Services. COMPANY may update its security practices from time to time but will not materially decrease the overall security of the Services during the term of the Agreement. COMPANY shall implement encryption measures for Personal Data both at rest and in transit to prevent unauthorized access. COMPANY shall maintain compliance with ISO 27001, SOC 2 Type 2, and PCI-DSS where applicable.

b. Personnel Background Checks. Prior to engaging any employee or contractor who may receive access to Personal Data COMPANY will conduct a background check subject to local laws.

c. Customer Responsibilities. The customer is responsible for security relating to its environment and databases and security relating its configuration of the Software. This includes implementing and managing procedural, technical, and administrative safeguards on its software and networks sufficient to: (a) ensure the confidentiality, security, integrity, and privacy of Customer Data in transit, at rest, and in storage; (b) protect against any anticipated threats or hazards to the security and integrity of Customer Data; and (c) protect against any unauthorized processing, loss, use, disclosure or acquisition of or access to Customer Data. Notwithstanding any other provision of this DPA, the Agreement or any other agreement related to the Software and Services, COMPANY will have no obligations or liability as to any breach or loss resulting from: (x) Customer's environment, databases, systems or software, or (y) Customer's security configuration or administration of the Software.

6 Information and Assistance.

a. Data Protection Impact Assessment. COMPANY will provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment that Customer may be required to perform under Data Protection Law.

b. Audit. If a Data Protection Law permits Customer to audit COMPANY's compliance with such law, COMPANY will assist Customer in satisfying the audit as follows. On Customer's request and subject to the confidentiality obligations set forth in the Agreement or an appropriate NDA, COMPANY will make available to Customer a summary of its most recent and relevant compliance certifications, as available, not more than once per year.

c. Questionnaires. If Customer requires additional information, COMPANY will respond to a reasonable and written Customer security questionnaire no more than once per year and meet by teleconference to address any additional questions.

d. Audit. If Customer requires additional information and reasonably believes COMPANY is not in compliance with this DPA or if required by a Supervisory Authority, Customer may contact COMPANY in accordance with the "Notices" Section of the Agreement to request an on-site audit, not more than once per year (unless required by a Supervisory Authority), of its procedures relevant to the protection of Personal Data.

e. Audit Procedure. At least two weeks before the commencement of any such on-site audit, Customer must provide to COMPANY a draft written audit plan, after which Customer and COMPANY shall discuss in good faith and finalize the audit plan and the parties shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for any travel or other expenses COMPANY incurs in the course of such audit. Audits may be conducted only during regular business hours, in accordance with the finalized audit plan and COMPANY's security and other policies, and may not unreasonably interfere with COMPANY's regular business activities. Customers shall promptly notify COMPANY with information regarding any non-compliance discovered during the course of an audit. Any third party engaged by Customer to conduct an audit must be pre-approved by COMPANY (such approval not to be unreasonably withheld) and sign COMPANY's confidentiality agreement.

f. Audit Results. Information obtained or results produced in connection with an audit are COMPANY Confidential Information under the Agreement and may only be used by Customer to confirm compliance with this DPA and for complying with its requirements under Data Protection Law.

7 Customer Security Measures.

a. Appropriate Permissioning. Customer is solely responsible for provisioning Authorized Users on the Software, including: (a) methods of authenticating Authorized Users (such as industry-standard secure username/password policies, two-factor authentication or SAML-supported SSO iDP); (b) restricting access by Authorized User or group, and from the database level down to the row or column level; (c) managing administrator privileges; (d) deauthorizing personnel who no longer need access to the Services; (e) securely configuring any APIs; and (e) regularly auditing any public access links Authorized Users create and restrict the permission to create public links, as necessary.

b. COMPANY Permission to Access Customer Databases. In order to use the Services, Customer must authorize the Services to access Customer's databases. When granting authorization, Customer must follow the principle of least privilege to Customer database information, especially by granting COMPANY no more than read-only access to database data. COMPANY will not be responsible for any Personal Data Breach, security incident, or other loss to the extent Customer provides the Services with write or administrator access to Customer's databases or other Personal

Data.

8 Data Breach Notification and Resolution.

a. Breach Notice. If it becomes aware of a confirmed Personal Data Breach, COMPANY shall inform Customer via email without undue delay. COMPANY shall further take any such reasonably necessary measures and actions to address or mitigate the effects of the Personal Data Breach and will keep Customer informed of all material developments in connection with the Personal Data Breach. The company's contact point for additional details regarding a Personal Data Breach is infosec@onebillsoftware.com. Except as required by applicable Data Protection Legislation, the obligations set out in this Section shall not apply to Personal Data Breaches caused by Customer.

b. Cooperation. Customer is solely responsible for complying with data incident notification requirements applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breach. COMPANY will provide reasonable information and cooperation to Customer so that Customer can fulfill any Personal Data Breach reporting obligations it may have under (and in accordance with the timescales required by) Data Protection Law. COMPANY's prior written approval shall be required for any statements containing specific information regarding COMPANY's systems, security practices, or the nature of the Personal Data Breach or references to COMPANY by name.

9 Miscellaneous.

a. Construction; Interpretation. This DPA is part of the Agreement and is governed by its terms and conditions (including limitations of liability. This DPA and the Agreement are the complete and exclusive statement of the mutual understanding of the parties and supersede and cancel all previous written and oral agreements and communications relating to the subject matter hereof. Headings contained in this DPA are for convenience of reference only and do not form part of this DPA. To the extent of any conflict between this DPA and the Agreement related to Personal Data, the DPA shall control. To the extent of any conflict between the Standard Contractual Clauses and the DPA, the Standard Contractual Clauses shall control.

b. Severability. If any provision of this DPA is adjudicated invalid or unenforceable, this DPA will be amended to the minimum extent necessary to achieve, to the maximum extent possible, the same legal and commercial effect originally intended by the parties. To the extent permitted by applicable law, the parties waive any provision of law that would render any clause of this DPA prohibited or unenforceable in any respect.

c. Amendment; Enforcement of Rights. No modification of or amendment to this DPA, nor any waiver of any rights under this DPA, will be effective unless in writing signed by the parties to this DPA. The failure by either party to enforce any rights under this DPA will not be construed as a waiver of any rights of such party. In the event Data

Protection Laws change subsequent to the signing of this DPA or the Agreement, the Parties shall negotiate in good faith to reach agreement on reasonable next steps, including, where applicable, changes that may be necessary and operationally, technically and commercially feasible to the Agreement, the DPA and/or the Services (including, without limitation, the fees payable by Customer to COMPANY for the Services) in order to enable COMPANY to continue providing the Services in compliance with such revised Data Protection Laws.

d. Business Transactions. COMPANY may share and disclose Personal Data and other Customer Data in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of COMPANY's business by or to another company, including the transfer of contact information and data of customers, partners and end users.

e. Bundling of Customer Entities. The parties agree that the bundling of Customer's data exporters, for example, if Customer is comprised of multiple global affiliates, as Controllers within this DPA is undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective Customer entity and COMPANY solely for purposes of addressing any such obligations under Data Protection Laws; (ii) shall not create any new or different legal or other relationship whatsoever between the "bundled" Customer entities; (iii) does not create any additional rights or remedies for such bundled Customer entities; (iv) all Processing instructions must be provided by the Customer entity that is signatory to the Agreement and COMPANY is not responsible for consolidating or evaluating the validity of instructions received from other Customer entities; (v) any commercial terms not provided by the DPA are provided by the Agreement regardless of whether the bundled Customer entities signed or were consulted regarding the terms of the Agreement; and (vi) any audits conducted in accordance with the DPA shall be conducted only by and through the Customer entity that is signatory to the Agreement.

f. Counterparts. This DPA may be executed and delivered by facsimile or electronic signature and in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

EXHIBIT A

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data Processor

Name:	The data processor is the entity identified as "Company" in the DPA
Address:	As set forth in the Agreement
Contact person:	General Counsel/Legal 3080 Olcott Street Suite D-230 Santa Clara, CA 95054 legal@onebillsoftware.com
Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA
Role:	"Company" acts solely as a Data Processor and does not determine the purposes or means of processing Personal Data. OneBill does not collect Personal Data independently and only processes data on behalf of the Customer, who acts as the Data Controller. The "Company" is responsible for ensuring that all Personal Data is lawfully collected and that appropriate legal bases for processing exist.

Data Controller

Name:	The data controller is the entity identified as "Customer" in the DPA
Address:	As set forth in the Agreement
Contact person:	As set forth in the Notices provision in the Agreement

Activities relevant to the data transferred under these Clauses:	As set forth in the Agreement
Signature and date:	Refer to DPA
Role:	As a Data Controller the "Customer" determines the purposes and means of processing personal data, deciding why and how the data should be processed. As part of its key responsibilities, the Data Controller defines the purpose of data processing, ensures compliance with applicable data protection laws, collects necessary consents when required, and is responsible for responding to data subject requests.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	"Authorized Users" as defined in the Agreement
Categories of personal data transferred:	Name Email address Cookie Information Device Identifiers, IP-address and other online identifiers Account log-in details and passwords Telephone/mobile number Location Data
Sensitive categories of data (if appropriate):	As determined and controlled by Customer in its sole discretion, and if provided to data processor, data processor shall comply with Section 2.9 of the DPA
The frequency of the transfer:	As set forth in the Agreement
Nature of the processing:	As set forth in Sections 2 of the DPA, and in the Agreement
Purposes of the data transfer and further processing:	As set forth in Sections 2 and 4 of the DPA, and in the Agreement

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 processed for the duration of the Agreement, subject to Section 2.7 of the DPA
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As set forth in Sections 2 and 4 of the DPA, and in the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

If Customer is established in an EU Member state, the competent supervisory authority shall be the supervisory authority applicable to the establishment location of Customer. If Customer is not established in an EU Member state, the competent supervisory authority shall be the supervisory authority located where Customer has appointed its EU Representative. If a Customer is not established in an EU Member state and is not required to appoint an EU Representative, the competent supervisory authority shall be the supervisory authority applicable to the location of the Data Subject whose data is at issue.

ANNEX II

Technical and organizational measures, including technical and organizational measures, to ensure the security of the data:

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

COMPANY uses reasonable technical and organizational measures designed to protect the Service and Customer Content as described in the OneBill Privacy Policy.

For transfers to Subprocessors, a description of the specific technical and organizational measures to be taken by the Subprocessor to be able to provide assistance to the Controller and, for transfers from a processor to a Subprocessor, to the data exporter:

The technical and organizational measures taken by the data importer to assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 are set out in Section 2f. (Cooperation and Data Subjects' Rights) of the DPA.

ANNEX III

List of Subprocessors:

Hosting service	AWS
Tax engines	Avalara, SureTax, Ceretax, Vertex,
Accounting	Quickbooks, Xero
Payment Gateways	Authorize.Net, Ippay, Stripe, Digitzs, Moneris, Paynetwork, Bambora, Cybersource, Worldpay, Braintree, Paypal, Korta, Valitor
PSA	Connectwise
Collaboration	Webex
CRM	Hubspot

EXHIBIT B – ADDITIONAL SCC PROVISIONS
BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS 01/2020

1. Company shall promptly notify Customer of any request for the disclosure of Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("Disclosure Request") unless otherwise prohibited by law or a legally binding order of such body or agency and without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). The company will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and to challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, the Company shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Company shall not disclose Personal Data requested until required to do so under applicable law. Company shall only provide the minimum amount of Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request. If the Disclosure Request is incompatible with the SCCs or other data transfer mechanism utilized in accordance with Section 3 in this DPA, Company will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Personal Data subject to the Disclosure Request. The company will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Company will provide Customer with such records relevant to Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Company's legal rights in connection with threatened, pending, or current litigation.
2. Company will utilize industry standard encryption while Personal Data is being Processed by Company.
3. Company has not purposefully created "back doors" or similar programming in its systems that provide Services that could be used to access the systems and/or Personal Data, nor has Company purposefully created or changed its business processes in a manner that facilitates access to Personal Data or its systems that provide the Services. To the best of Company's knowledge, United States Data Protection Law does not require Company to create or maintain "back doors" or to facilitate access to Personal Data or systems that provide Services or for Company to possess or provide the encryption key in connection with a United States Disclosure Request.
4. Company shall use reasonable efforts to assist Customer and its Data Subjects, as instructed by Customer (in accordance with Section 2 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Customer in connection with the Data Subject's efforts to exercise its rights and obtain legally available redress, provided Company shall not be required to provide Customer or Data Subjects with legal advice.
5. Customers may request to audit Company access logs regarding access to Personal Data, subject to the terms of Section 6 of the DPA.
6. The company has established an internal policy and procedure regarding handling of Disclosure Requests and applicable transfers of Personal Data of customers. Company Legal and Audit personnel are provided information regarding applicable transfers of Personal Data

prior to the transferring of any such data, where such information may include an explanation of the necessity of the transfer and any data protection safeguards in scope.

7. In the event Company receives a request to voluntarily disclose unencrypted Personal Data to a government authority, Company will use reasonable efforts to first obtain Customer's consent, either on its behalf or on behalf of the relevant Data Subject.