# BILLTRUST DATA PROCESSING ADDENDUM

This Billtrust Data Processing Addendum (this "**Addendum**"), including all its exhibits, is entered into by and between Factor Systems, LLC d/b/a acting on its own and as agent for the Billtrust Affiliates (collectively referred to as "**Billtrust**") and the customer agreeing to these terms (the "**Customer**") (each, a "**Party**" and, collectively, the "**Parties**"). This Addendum (including its exhibits) form part of the Agreement (as defined in section 1 below) between Billtrust or a Billtrust Affiliate and Customer. This Addendum replaces any data processing agreement that was previously concluded between the Customer and Billtrust.

This Addendum sets out obligations of the Parties with respect to data protection in relation to the Agreement. To the extent of any conflict or inconsistency between the provisions of this Addendum (including any annexes and appendices thereto) and any provision of the Agreement, the provisions of this Addendum shall prevail and take precedence over such conflicting or inconsistent provisions in the Agreement as set forth below in Section 8.3. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum and its exhibits.

**RECITALS**

**WHEREAS**, the Parties entered into the Agreement and have retained the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement;

**WHEREAS**, in the course of providing its services under the Agreement, Billtrust, as a Data Controller or as a Data Processor, Processes certain Personal Data of Data Subjects;

**WHEREAS**, Customer, as a Data Controller, requires that its service providers who may Process Personal Data shared with them by Customer, take all necessary measures to handle such information in compliance with Applicable Data Protection Laws; and

**WHEREAS**, the Parties now wish to supplement the Agreement to ensure that Personal Data (as defined below) transferred between the Parties is Processed in accordance with Applicable Data Protection Laws.

**NOW, THEREFORE**, in consideration of the mutual agreements set forth in this Addendum, the Parties agree as follows:

**TERMS**

## 1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement(s). Except as modified or supplemented below, the definitions of the Agreement shall remain in full force and effect.

1.2. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

(a) "**Agreement**" includes any agreement for the provision of Controller Services or Processor Services.

(b) "**Applicable Data Protection Laws**" means all laws that are applicable to the Processing of Personal Data under the Agreement specified in **Exhibit B** hereto;

(c) "**Billtrust Affiliates**" means any companies which are controlled by BTRS Holdings Inc, which control Billtrust or which are under common control with Billtrust and either: (i) are Controllers of any Personal Data; and/or (ii) on whose behalf Vendor and/or any Sub-Processor otherwise processes any Personal Data. For these purposes "control" and its derivatives means to hold, directly or indirectly, more than 50% of the respective shares with voting rights.

(d) "**EEA Data Protection Laws**" means the GDPR and laws implementing or supplementing the GDPR;

(e) "**Customer Personal Data**" means any Personal Data Processed by Billtrust pursuant to or in connection with the Agreement(s), as applicable;

(f) "**Controller Services**" means the Credit Subscription Services, the Business Payment Network, and the Business Directory under the Agreement, any other services for which Billtrust would factually act as a Controller, and Billtrust marketing activities as described under the Agreement;

(g) "**Effective Date**" means the date the Parties entered into the controlling Agreement, as defined in the Agreement;

(h) "**GDPR**" means 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, and repealing Directive 95/46/EC;

(i) "**Personal Data Recipient**" means Billtrust, a Sub-processor, or both collectively;

(j) "**Restricted Transfer**" means any transfer of Personal Data to a third country or an international organization that would be prohibited by Applicable Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Data Protection Laws) in the absence of the execution of the Standard Contractual Clauses or another lawful data transfer mechanism, as set out in **Jurisdiction Specific Terms** hereto below;

(k) "**Services**" means the services and other activities carried out by or on behalf of Billtrust for Customer pursuant to the Agreement.

(l) "**Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914, including the European Commission Decision C(2004)5721, SET II, Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers), or European Commission Decision C(2010)594, Standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as applicable to each Party's controllership role and geographic location for the relevant Processing activity (and as updated from time to time if required by law or at the choice of Billtrust to reflect the latest version adopted by the European Commission). **Exhibit A** provides the required Annex information to support the applicable Standard Contractual Clauses.

(m) "**Processor Services**" means all Services under the Agreement which are not Controller Services and any other services for which Billtrust would factually act as a Processor on behalf of Customer;

(n) "**Sub-processor**" means any third party appointed by or on behalf of Billtrust to Process Personal Data on behalf of Customer in connection with the Agreement;

(o) "**Supervisory Authority**" includes any competent authority tasked with the enforcement of the Applicable Data Protection Laws.

(p) "**Terms**" means Section 1 to 11 of this Addendum.

1.3. The terms "**Data Controller**" or "**Controller**", "**Data Subject**", "**Data Processor**" or **"Joint Controller**", "**Processor**", "**Recipient**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Sub-Processor**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. For the purposes of this Addendum, Data Controller or Data Controllers, Data Processor or Data Processors, Data Importer, and Data Exporter also refers specifically to a Party or the Parties to this Addendum.

## 2. Scope

2.1. This Addendum serves as a framework for Personal Data Processing under the Agreement, as well as Personal Data sharing between the Parties as Data Controllers or when Billtrust is a Data Processor or Sub-Processor acting on the instructions of Customer, when applicable, and defines the principles and procedures that the Parties shall adhere to and the respective responsibilities of the Parties.

2.2. This Addendum will apply to the Processing of all Personal Data, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor, to the extent that such Processing falls under the material and territorial scope of the Applicable Data Protection Laws.

## 3. Roles of the Parties and Applicability of the Controller to Controller Terms, the Controller to Processor Terms and the Remaining Sections of the Addendum

3.1. **Controller Services:**

The Terms of this Addendum shall be supplemented by section 3.2 of this Addendum when:

(a) In the context of this Addendum and its exhibits, with regard to the Processing of Personal Data in the context of the provision of the Controller Services, Customer and Billtrust both act as Controllers; in which case, Customer is a controller and Billtrust is an independent controller, not a joint controller with Customer.

(b) and to the extent that, Billtrust acts as a Controller in the context of this Addendum.

3.2. **Controller to Controller Terms**

With respect to the Controller Services, each Party represents, warrants, and covenants that:

(a) it is a Data Controller as to Personal Data with respect to the Processing of Personal Data under the Agreement, as applicable;

(b) all Personal Data will be collected, transferred, and otherwise Processed in accordance with the applicable laws, including Applicable Data Protection Laws as they apply to each Party, respectively;

(c) it will, upon request of the respective other Party, provide that other Party with copies of all relevant data protection laws or references to them (where relevant, and not including legal advice); and

(d) it is not aware of the existence of any local laws that would have a substantial adverse effect on the obligations provided for under this Addendum.

With respect to the Controller Services, each Party agrees that:

(e) Processing is limited to that which is reasonably necessary to perform the Services under the applicable Agreement(s).

(f) the Processing of Customer Personal Data for the purposes set out in the Service Agreement(s) shall be performed only on lawful grounds, as provided by Applicable Data Protection Laws including, without limitation, Article 6 of the GDPR, as further limited by Article 9 of the GDPR, as applicable.

(g) persons they authorize to Process Customer Personal Data must have committed themselves to confidentiality or be under an appropriate statutory or professional obligation of confidentiality.

(h) Customer Personal Data will not be further processed in a manner that is incompatible with the purposes for which it was originally collected by the Data Controller sharing the Personal Data.

(i) To the extent that a disclosure of Customer Personal Data among the Data Controllers qualifies as a sale under Applicable Data Protection Laws, each Data Controller must comply with the obligations associated with the sale of Personal Data under the relevant Applicable Data Protection Laws.

3.3. **Processor Services:**

The Terms of this Addendum shall be supplemented by the section 4.4 of this Addendum when:

(a) In the context of this Addendum and its exhibits, with regard to the Processing of Personal Data in the context of the provision of the Processor Services:

i. when Customer acts as a Controller, Billtrust acts as a Processor; and

ii. when Customer acts as a Processor, Billtrust acts as a Sub-Processor.

For the avoidance of doubt, both situations fall within the scope of and are covered by this Addendum.

(b) and to the extent that, Billtrust acts as a Processor or a Sub-Processor in the context of this Addendum.

3.4. **The Processor Terms**

**(a) Billtrust shall:**

i. comply with all applicable laws in the Processing of Customer Personal Data, including Applicable Data Protection Laws;

ii. not Process Customer Personal Data other than on Customer's relevant documented instructions (including with regard to international transfers of Personal Data), unless such Processing is required by applicable laws to which the relevant Personal Data Recipient is subject, in which case Billtrust shall, to the extent permitted by applicable laws, inform

Customer of that legal requirement before the respective act of Processing of that Personal Data;

iii. only conduct transfers of Customer Personal Data in compliance with all applicable conditions, as laid down in Applicable Data Protection Laws;

iv. not retain, delete, or otherwise Process Personal Data contrary to or in the absence of the direct instructions of Customer, provided, however, that Customer expressly and irrevocably authorizes such retention, deletion or other Processing if and to the extent required or allowed by Applicable Laws; and

v. immediately inform Customer in the event that, in Billtrust's opinion, a Processing instruction given by Customer may infringe applicable laws.

**(b) Customer shall:**

i. provide all information which is applicable to the Customer, as provided in Exhibit A, attached hereto and incorporated by reference, and keep all such information complete and up to date.

ii. Instruct Billtrust (and authorize Billtrust to instruct each Sub-processor) to Process Customer Personal Data, and in particular, transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum.

iii. represent and warrant that it has all necessary rights to provide Customer Personal Data to Billtrust for the purpose of Processing such data within the scope of this Addendum and the Agreement. Within the scope of the Agreement(s) and in its use of the Services, Customer shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Customer Personal Data to Billtrust and the Processing of Personal Data.

**(c) Billtrust Personnel**

i. Billtrust shall take reasonable steps to strictly limit access to Customer Personal Data to those individuals who need to know or access it, as strictly necessary to fulfil the documented Processing instructions given to Billtrust by Customer or to comply with applicable laws.

ii. Billtrust shall require that all individuals covered by this section are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

**(d) Security of Processing**

i. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing, as well as the risk of varying likelihood and severity to the rights and freedoms of natural persons, Billtrust shall, with regard to Customer Personal Data, implement and maintain appropriate technical and organizational security measures to provide a level of security appropriate to that risk, as well as assist Customer with regard to ensuring compliance with Customer's obligations pursuant to the Applicable Data Protection Laws as referenced under **Exhibit B** to this Addendum

ii. Customer acknowledges that the security measures are subject to technical progress and development and that Billtrust 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 purchased by Customer.

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

**(e) Use of Sub-Processors**

i. Customer authorizes Billtrust to appoint (and permit each Sub-Processor appointed in accordance with this Section 9 to appoint) Sub-Processors in accordance with this Section 4 and any possible further restrictions, as set out in the Agreement, as the case may be.

ii. Billtrust may continue to use those Sub-Processors already engaged by Billtrust as of the date of this Addendum, subject to Billtrust meeting the obligations set out this Section 4. The list of Billtrust's Sub-processors is available at https://www.billtrust.com/sub-processors/.

iii. Billtrust shall provide Customer prior written notice of the appointment or replacement of any new Sub-Processor by offering Customers a mechanism to subscribe to updates to the list of Billtrust Sub-Processors. Within 30 days of posting of each such notice, Customer may object to the appointment or replacement of a sub-processor provided such objection is in writing and based on reasonable grounds relating to data protection.

iv. With respect to each Sub-processor, Billtrust shall:

- carry out adequate due diligence to ensure that the Sub-processor is capable of providing the level of protection and security for Personal Data required by this Addendum, the Agreement, and Applicable Laws before the Sub-processor first Processes Personal Data or, where applicable, in accordance with Section 3.4; and
- impose terms between Billtrust and the prospective Sub-processor that offer at least the same level of protection for Personal Data as those set out in this Addendum on the Sub-processor and meet the requirements of Applicable Data Protection Laws.

**(f) Rights of the Data Subjects**

i. Taking into account the nature of the Processing, Billtrust shall assist Customer by establishing and maintaining commercially reasonable appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise rights of the Data Subjects under Applicable Data Protection Laws.

ii. With regard to the rights of the Data Subjects within the scope of Section 3.4, Billtrust shall:

- promptly notify Customer if any Personal Data Recipient receives a request from a Data Subject with respect to Personal Data; and

- not substantively respond to that request and direct any Personal Data Recipients not to respond to that request, except on the documented instructions of Customer, or as required by Applicable Data Protection Laws to which the Personal Data Recipient is subject, in which case Billtrust shall, to the extent permitted by Applicable Laws, inform Customer of that legal requirement before the Personal Data Recipient responds to the request.

**(g) Personal Data Breach**

i. Billtrust shall notify Customer without undue delay upon Billtrust becoming aware of a Personal Data Breach affecting Customer Personal Data under Billtrust's direct control or upon Billtrust being notified of a Personal Data Breach affecting Customer Personal Data under the direct control of a Sub-processor, providing Customer with the requisite information as per the Applicable Data Protection Laws.

ii. Billtrust shall cooperate with Customer and take all reasonable commercial steps to assist Customer in the investigation, mitigation, and remediation of each such Personal Data Breach.

iii. Billtrust's notification of or response to a Personal Data Breach under this Section 6 will not be construed as an acknowledgement by Billtrust of any fault or liability with respect to the Personal Data Breach.

**(h) Data Protection Impact Assessment and Prior Consultation**

i. Billtrust shall provide Customer with relevant information and documentation, such as, if available, an audit report (upon a written request and subject to obligations of confidentiality), with regard to any data protection impact assessments, and prior consultations with supervisory authorities when the Customer reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Laws. Such information and documentation shall pertain solely to Processing of Customer Personal Data by the respective Personal data recipient and shall take into account the nature of the Processing and the information available to the respective data recipient.

**(i) Deletion or Return of Personal Data**

i. Billtrust shall provide Customer with the technical means, consistent with the way the Services are provided, to request the deletion of Customer Personal Data upon the request of Customer unless applicable laws require storage of any such Customer Personal Data.

ii. Following the date of cessation of Services involving the Processing of Customer Personal Data, at the Customer's request, Billtrust shall delete or return all Personal Data to Customer, unless Applicable Laws require storage of any such Personal Data. In case the Agreement contains specific provisions for this situation, the provisions of the Agreement shall prevail provided they comply with Applicable Data Protection Laws.

**(j) Audit Rights**

i. Where Customer is entitled to and desires to review Billtrust's compliance with the Applicable Data Protection Laws, Customer may request, and Billtrust will provide (subject to obligations of confidentiality) relevant documentation, or any relevant audit report Billtrust might have

issued. If Customer, after having reviewed such audit report(s), still reasonably deems that it requires additional information, Billtrust shall further reasonably assist and make available to Customer, upon a written request and subject to obligations of confidentiality, all other information (excluding legal advice and commercially sensitive information (e.g. relating to pricing)) and/or documentation necessary to demonstrate compliance with this Addendum, and the obligations pursuant to the Applicable Data Protection Laws (Articles 32 to 36 of the GDPR in particular).

ii. Upon reasonable prior notice, Billtrust shall allow for and contribute to audits, including remote inspections of the Services, by Customer or an auditor mandated by Customer with regard to the Processing of the Personal Data by Billtrust. Billtrust shall provide the assistance described in this Section 3(j) insofar as in Billtrust's reasonable opinion such audits, and the specific requests of Customer, do not interfere with Billtrust's business operations or cause Billtrust to breach any legal or contractual obligation to which it is subject. Any audits conducted on Billtrust premises shall be conducted during normal business hours and shall be conducted in a way such as to cause minimal business disruption.

iii. Customer shall not conduct such audit more than once per year, unless (i) when required by instruction of a competent data protection authority or (ii) when Customer believes a further audit is necessary due to a Personal Data breach suffered by Billtrust.

3.5. The Terms of the Addendum (including its exhibits) are applicable regardless of the role of the Parties, unless, and to the extent that, a specific Section indicates the contrary.

**4. Records of Processing Activities**

4.1. Each Party agrees to maintain a record of Processing Activities of Customer Personal Data under its responsibility, as required by Applicable Data Protection Laws.

**5. International Data Transfers**

5.1. International transfers of Customer Personal Data within the scope of this shall be conducted in accordance with the applicable terms and conditions of **Exhibit B**.

5.2. Where the Standard Contractual Clauses are the applicable data transfer mechanism according to the terms and conditions set out in **Exhibit B**, the applicable Standard Contractual Clauses will be the clauses applicable to the role of the Parties as set out in **Exhibit A** of the Addendum.

5.3. For avoidance of doubt, by entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses and **Exhibit B** incorporated herein, including their Annexes, as of the Effective Date.

**6. Exhibits to the Addendum**

6.1. Jurisdiction Specific Terms:

(a) To the extent the Parties Process Customer Personal Data originating from, or protected by, Applicable Data Protections Laws in one of the jurisdictions listed in **Exhibit B** ("**Jurisdiction Specific Terms**"), then the terms specified in **Exhibit B** with respect to the applicable jurisdiction(s) shall apply in addition to the Terms of this Addendum and the appropriate Module. For the avoidance of doubt,

the Jurisdiction Specific Terms do not apply to the Processing if Customer Personal Data does not originate, or is protected by Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit B**.

(b) Billtrust may update **Jurisdiction Specific Terms** from time to time to reflect changes in or additions to Applicable Data Protection Laws to which the Parties are subject. Billtrust shall provide Customer prior written notice of any changes to **Jurisdiction Specific Terms** by offering Customers a mechanism to subscribe to a notification system of updates as posted on the Billtrust website. If Customer does not object to the updated **Jurisdiction Specific Terms** within thirty (30) days of receipt, Customer will be deemed to have consented to the updated **Jurisdiction Specific Terms**.

(c) In case of any conflict or ambiguity between the **Jurisdiction Specific Terms** and any other terms of this Addendum, the applicable **Jurisdiction Specific Terms** will prevail.

6.2. Updates Related to Restricted Transfers:

(a) Billtrust may update **Exhibits A and C** from time to time to reflect changes in or additions necessary to conclude the Standard Contractual Clauses.

## 7. Indemnification

7.1. Customer agrees to indemnify and hold harmless Billtrust and its officers, directors, employees, agents, affiliates, successors, and permitted assigns against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind which Billtrust may sustain as a consequence of the breach by Customer of its obligations pursuant to the Applicable Data Protection Laws or this Addendum.

## 8. General Terms

8.1. This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between the Billtrust and Customer.

8.2. All clauses of the Agreement that are not explicitly amended or supplemented by the clauses of this Addendum remain in full force and effect and shall apply, as long as this does not contradict with compulsory requirements of Applicable Data Protection Laws under this Addendum.

8.3. In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this Addendum, the provisions of this Addendum shall prevail. This is without prejudice to the order of precedence between the Jurisdiction Specific Terms and any other provision in this Addendum as set out in Section 6.1 (c) above.

8.4. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Addendum will continue in effect.

8.5. If Billtrust makes a determination that it can no longer meet any of its obligations in accordance with this Addendum, its Exhibits or the Standard Contractual Clauses (where applicable), or under Applicable Data Laws, it shall promptly notify Customer of that determination, and cease the Processing of Customer Personal Data or take other reasonable and appropriate steps to remediate.

8.6. If you are accepting the terms of this Addendum on behalf of an entity, you represent and warrant to Billtrust that you have the authority to bind that entity and its affiliates, where applicable, to the terms and conditions of this Addendum.

8.7. This Addendum and its exhibits is governed by the laws that apply to the Agreement. Any disputes between the Customer and Billtrust as a result of the creation, fulfillment, and/ or interpretation of the Addendum shall be exclusively submitted to the courts appointed as per the Agreement.

**9. Data Protection Representative Representative(s)**

9.1. The UK Representative of Billtrust pursuant to Article 27 of the UK GDPR is:

VeraSafe United Kingdom Ltd.
37 Albert Embankment
London SE1 7TL
United Kingdom

Contact form: https://www.verasafe.com/privacy-services/contact-article-27-representative/

**10. Liability**

10.1. Without prejudice to any form of direct liability of a Party to Data Subjects, subject to the limitations set forth in the Agreement(s), each Party shall be liable to the other respective non-defaulting Party for damages the defaulting Party has caused to the non-defaulting Party by any breach of its obligations, as set out in this Addendum.

**11. Termination**

11.1. This Addendum (including its Exhibits) shall be effective for the entire term of the Agreement and it shall terminate automatically upon expiry or termination of the Agreement, except for those provisions that, by nature, must survive termination of the Addendum.

# Exhibit A: SCC's Appendices and Details of Processing

## A. List of Parties

**DATA EXPORTER: The Customer entity identified in the Agreement and Addendum with an address as set forth in the Agreement.**

Contact details:, see heading section of this Addendum for additional details.

Activities relevant for the Addendum: to provide the Services pursuant to the Agreement.

**DATA IMPORTER: The Billtrust entity identified in the Agreement and this Addendum with an address as set forth in the Agreement.**

Contact details: privacy@billtrust.com; see heading section of this Addendum for additional details.

Activities relevant for the Addendum: to receive the Services set out in the Agreement.

**ROLES**:

- Where Customer is acting as Data Controller and Data Exporter and Billtrust is acting as a Data Controller and Data Importer: see Processing Annex 1
- Where Customer is acting as Data Controller and Data Exporter and Billtrust is acting as a Processor: see Processing Annex 2
- Where Customer is acting as Data Processor and Data Exporter and Billtrust is acting as a Sub-Processor: see Processing Annex 2

## B. Description of Transfer

This section sets out the Processing Annexes concerning Personal Data transferred to a third country by the Parties pursuant to the Agreement. The Parties may agree additional Processing Annexes from time to time in accordance with the terms of the Agreement. There are three categories of data envisaged by this Agreement, set forth in two processing annexes as follows:

- Processing Annex 1: Controller to Controller
- Processing Annex 2: Controller to Processor, Processor to Sub-Processor

| **Processing Annex 1: Controller to Controller** | | | |
|---|---|---|---|
| **Product** | **BPN** | **Credit** | **BBD** |
| **Data Subjects** The Personal Data transferred | - Customers (past, current and prospective) of Billtrust, also referred to as "Suppliers". | Sole proprietors who are customers of Billtrust's Customers. | Sole proprietors who are customers of Billtrust's Customers |

| | | | |
|---|---|---|---|
| concerns the following categories of data subjects: | - Sole proprietors who are customers of Billtrust's Customers.<br>- staff of past, present and potential users of Billtrust Services | | |
| **Categories of Personal Data Transferred** | First and last name, email address, company address, Tax ID (which can be a Social Security Number), account name and name of account owner(s), and Merchant ID; telephone number, bank account information (to facilitate ACH and wire transactions); monthly check data/volume, transaction value of payments flowing through the BPN (ultimately, this data is aggregated); supplier's payment preferences. | First and last name, business address, email address, Federal Tax ID (which can be a Social Security Number), shipping address, username (and password), financial statements, trade data, business operational, employment and financial characteristics; government compliance data; credit or exposure and payment experiences; industry opinions; job title; any content that the data subject creates or shares, including any communications with Credit or other users, and other information related to the data subject's work or organization. | Company name (such as sole proprietor's name), email address.<br><br>Number of electronic payments, number of payments with paper checks, payment preferences (paper checks/electronic payment) (this is further aggregated). |
| **Sensitive Personal Data Transferred (If applicable)** | n/a | n/a | n/a |
| **The frequency of the transfer** | continuous basis | continuous basis | continuous basis |
| **Nature of the processing** | To create a two-sided platform in which payable providers can deliver digital payments directly to the suppliers' acceptance platforms. | To gather and analyze credit application information for Billtrust Customers. | To identify opportunities within Billtrust Customers' customer bases to convert print invoices to electronic invoices and payments from paper checks to online payments. |

| | | | |
|---|---|---|---|
| **Purposes of the transfer(s)** | To maintain or service accounts for Billtrust Customers, to provide customer service to Billtrust Customers, to process or fulfill order processing and transactions including ACH and wire transfers, to verify customer information, to process payments made by customers of Billtrust's Customers, and providing the Business Payment Network product to Billtrust Customers; to contact Billtrust Customers, when required. | To create global business profiles, to enable portfolio monitoring and to send alerts on portfolio accounts of Billtrust's Customers, and to create a portal that gathers credit application information, as part of the credit onboarding decision process of Billtrust's Customers; | To provide Billtrust Customers with aggregated information of their end-customers who are online payment users. |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** | For the period necessary to fulfil the purposes outlined above unless a longer retention period is required or permitted by law, for legal, tax or regulatory reasons, or other lawful legitimate purposes. | For the period necessary to fulfil the purposes outlined above unless a longer retention period is required or permitted by law, for legal, tax or regulatory reasons, or other lawful legitimate purposes. | For the period necessary to fulfil the purposes outlined above unless a longer retention period is required or permitted by law, for legal, tax or regulatory reasons, or other lawful legitimate purposes. |
| **Transfers** The Personal Data transferred may be disclosed to the following recipients or categories of recipients: | Payment gateways<br>Service providers who provide:<br>● cloud data storage services and SaaS-based integration platforms<br>● co-location and infrastructure services<br>● payment infrastructure platforms | Credit bureaus<br>Credit analysts<br>Factoring organizations<br>Other Billtrust's customers<br>Service providers who provide:<br>● hosting services<br>● cloud data storage services and SaaS-based integration platforms<br>● cloud-computing software<br>● co-location and infrastructure services | Billtrust to Customer to deliver the Services pursuant to the Agreement. |

| | | | |
|---|---|---|---|
| | • ACH wire transaction facilitators<br>• business intelligence software<br>• big data analytics platform<br>• event logging platforms | • electronic signature software<br>• anti-money laundering solutions<br>• payment infrastructure platforms<br>• ACH wire transaction facilitators<br>• business intelligence software<br>• big data analytics platform<br>• event logging platforms<br>• security solutions<br>• interactive voice response systems | |

| **Processing Annex 2: Controller to Processor and Processor to Processor** | |
|---|---|
| **Categories of data subjects whose personal data is transferred** | Data Exporter's personnel<br>Data Exporter's customers personnel<br>Data exporter's users of the Services |
| **Categories of personal data transferred** | Categories of personal data transferred are defined in the Agreement; e.g. identifiers and commercial information, including email address, first and last name, login credentials, employer, job title, credit card company, credit card number and expiration date, credit card billing address, bank account information, invoicing information.<br>Customer shall ensure not to provide any data (i) containing sensitive personal data (as listed in article 9.1 of the GDPR), (ii) related to criminal activities (as listed in article 10.1 of the GDPR), or (iii) containing national identifiers which are considered sensitive personal data subject to applicable legislation. |
| **Sensitive data transferred** | n/a |
| **The frequency of the transfer** | Data will be transferred on a continuous basis subject to the terms of the Agreement(s), in the context of the contractual relationship between Billtrust and the Customer. |
| **Nature of the processing** | Processing pertains to the provision of the Processor Services under the Agreement.<br>Processing operations to which the Personal Data will be subject include, without limitation: |

| | |
|---|---|
| | collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, alignment, or combination, blocking, erasure, or destruction. |
| **Purpose(s) of the data transfer and further processing** | The purpose of processing of personal data pertains to the provision of specified products and services under the Agreement(s). |
| **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** | For the duration of the Agreement between Data Exporter and Data Importer and in accordance with the Addendum including section 3.4(i). |
| **For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing** | Where the Data Importer engages Processors (or sub-Processors) it will do so in compliance with the terms of the Standard Contractual Clauses. The subject matter, nature and duration of the Processing activities carried out by the Processor (or Sub-Processor) will not exceed the Processing activities as described in the Agreement. |

**C. <u>Security Measures</u>**

a. Customer acknowledges and agrees that Billtrust may change its security policies and related security measures, provided that Billtrust maintains, at all times, an overall level of security as least as stringent as the one set forth in this Addendum.
b. For the avoidance of doubt, to the extent of any conflict or inconsistency between the provisions of this Addendum and any of the Security Measures listed below, the Security Measures shall prevail and take precedence over such conflicting or inconsistent provisions in this Addendum, subject to Section 8.3 above.
c. Billtrust Processes Personal Data in accordance with applicable law to which Billtrust is subject and in accordance with the data security requirements of the controls defined by latest available SSAE 18 SOC 1/2 or ISO 27001 implemented controls (or equivalent standard).

d. Comprehensive security policies, standards and procedures are developed and maintained by a designated person responsible for privacy and data protection and reviews of the information security policy are completed at least annually.
e. Billtrust provides its personnel, third party consultants, and contractors with annual information security awareness training including, but not limited to, education on general security awareness, relevant security policies and procedures, and Personal Data Processing.
f. Billtrust agrees to maintain suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment (namely database and application servers and related hardware) where the Personal Data is Processed or used.
g. Physical Security
    i. The equipment hosting the application for Customer is located in a physically secure facility, which requires badge access at a minimum.
    ii. Physical access to infrastructure housing Customer's content is restricted and access allowed based on a need-to-know basis.
    iii. Electronic media (online or offline) and confidential hard copy material is appropriately protected from theft or loss.
h. Authentication
    i. All access to Billtrust systems is controlled by an authentication method involving a minimum of a unique User ID/complex password combination.
    ii. Privileged users and administrators use strong authentication.
    iii. Passwords are changed every ninety (90) days.
    iv. Passwords are never to be stored in clear text.
    v. Passwords are complex and not easy to guess or crack. Effectiveness of authentication is tested on a regular basis to verify that unauthorized authentication is not easily permitted.
    vi. Remote network access is secured by strong authentication.
    vii. All activity performed under a User ID is the responsibility of the individual assigned to that User ID. Users do not share their User ID/password with others or allow other employees to use their User ID/password to perform actions.
    viii. Use of generic user account is not to be permitted.
i. Authorization
    i. Logical or network access to infrastructure housing Customer Data is restricted and access allowed based on a need-to-know basis.
    ii. Access requests are documented and approved based on a business need.
    iii. Access rights are reviewed on a periodic basis.
    iv. Upon termination or resignation of personnel, access is revoked within a timely manner.
j. Change Management
    i. Change requests are documented via ticketing system. The process to review and approve change requests must be documented. The change request contain, at a minimum, the following information:
        1. Business justification for the change
        2. Nature of defect (if applicable)/enhancement
        3. Testing required
        4. Back-out procedures
        5. Systems affected
        6. User contact
        7. Management approval
k. Network Security

i. Industry standard firewalls are implemented to protect the application environment and associated data from the Internet and untrusted networks.
ii. Inbound and outbound connections are denied unless expressly allowed.
iii. Firewall events are monitored in order to detect potential security events.
iv. Network Intrusion Detection or Prevention Systems (NIDS/NIPS) are implemented to monitor traffic for applications handling Confidential Information.
v. Effectiveness of controls are tested on a periodic basis.

l. Logging and Monitoring
i. Security relevant events, including, but not limited to, login failures, use of privileged accounts, changes to access models or file permissions, modification to installed software, or the operating system, changes to user permissions, or privileges or use of any privileged system function, are logged on all systems.
ii. Billtrust maintains electronic logs of access to sensitive information that depict the details of the access.
iii. Billtrust maintains a security logging and monitoring process which identifies potential security violations in near-real time.
iv. Logs shall be regularly (with the period commensurate with risk) reviewed by Billtrust, either manually or using log parsing tools. Billtrust uses automated alerts to detect security events and security alerts are communicated to authorized personnel to appropriately handle alerts.

m. System and Data Security
i. Systems are securely configured according to a security baseline. This baseline includes removing unnecessary services and changing default, vendor-supplied or otherwise weak user accounts and passwords.
ii. System components maintain current security patch levels.
iii. Web servers are hardened according to a secure baseline.
iv. Web servers are configured to accept requests for only authorized and published directories.
v. Default sites, executable or directory listings are disabled.
vi. An inventory of technology used to store or process Customer Data is maintained.
vii. Billtrust implements industry standard anti-virus/malware software operating in real time on all servers, laptops and desktops.
viii. All Customer Data is encrypted while in transit and at rest.
ix. Billtrust encrypts sensitive information that traverses networks outside of the direct control of Billtrust (including, but not limited to, the internet, Wi-Fi and mobile phone networks).
x. Billtrust applies the “Principle of Least Privilege” (“PLP”) model, enabling access only to such sensitive non-public information and other rights and privileges relating to Customer as are necessary for Billtrust to perform a legitimate business function.
xi. Billtrust utilizes the following application management controls:
1. Maintains a software development life cycle (“SDLC”) process that incorporates security vulnerability and malicious code assessments throughout each stage of the development process.
2. Billtrust provides regular training on coding and design in application security.
3. Within Billtrust’s SDLC, a security vulnerability and malicious code assessment is performed prior to initial application deployment.
4. Application development activities do not occur on Billtrust’s systems that also perform live production operations.

5. Application source code is permanently stored on systems dedicated to the storage of source code (such as a source code repository) that includes logs of all updates to code maintained. Permanent storage of source code on laptops, desktops and other mobile computing devices is prohibited.
6. Access to the application source code is limited to Billtrust employees in accordance with PLP.
7. Application source code is maintained using version control.
8. Application documentation is kept up to date, held in accessible form, and protected from loss or damage.
9. Information security requirements are integrated with the design and specification documentation for Billtrust's systems.
10. Billtrust subjects its operating system, software and firmware updates to a security review to screen for vulnerabilities and to verify the source of the items, prior to implementation, and is able to validate that the update is from an approved source.
11. Billtrust performs security testing of application open source code, and remediates security flaws prior to production implementation.

n. Billtrust will conduct security testing consistent with industry standards for all software developed or customized for Customer and remediates any security flaws identified.
o. Billtrust develops web applications in compliance with Open Web Application Security Project ("OWASP") application security verification standard. Web Applications are reviewed for the presence of the OWASP top ten.
p. Billtrust will remediate security flaws and vulnerabilities identified in application security tests in accordance with Billtrust's vulnerability management processes.

**D. <u>List of Sub-Processors</u>**

a. Billtrust is a Data Processor (and where the Controller to Processor OR Processor to Processor SCCs apply); the controller has authorised the use of the following sub-processors: https://www.billtrust.com/sub-processors/

**E. <u>Competent Supervisory Authority</u>**

a. The competent Supervisory Authority shall be determined as follows:
    i. Where Billtrust is established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of that EU Member State in which Billtrust is established.
    ii. Where Billtrust is not established in an EU Member State: the competent Supervisory Authority shall be the Supervisory Authority of the Netherlands.

# Exhibit B: Jurisdiction-Specific Terms

**1. Transfers of EEA Personal Data**

1.1. Definitions:

(a) For the purpose of interpreting the Addendum, the following terms shall have the meanings set out below:

i. "**EEA**" means the European Economic Area.

ii. "**EEA Restricted Transfer**" includes any transfer of Personal Data subject to the GDPR (including data storage on foreign servers) which is undergoing Processing or is intended for Processing after transfer, to a Third Country (as defined below) or to an international organization.

iii. "**Supervisory Authority**" in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

iv. "**Third Country**" (as used in this Section) means a country outside of the EEA.

1.2. Transfer Mechanisms:

(a) With regard to any EEA Restricted Transfer from Customer to Billtrust within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision pursuant to the requirements under the GDPR that provides that the Third Country, a territory or one or more specified sectors within that Third Country, or the international organization in question to which Customer Personal Data is to be transferred ensures an adequate level of data protection;

ii. Billtrust's certification to any successor to the Privacy Shield Framework, including but not limited to the EU – U.S. Data Privacy Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the GDPR, as the case may be), provided that the Services are covered by the self-certification, if applicable;

iii. the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the GDPR, as the case may be); or

iv. any other lawful basis, as laid down in the GDPR, as the case may be.

1.3. Standard Contractual Clauses:

(a) The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in Exhibit C to this Addendum serves to supplement the Standard Contractual Clauses.

(b) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

(c) **Module One:** To the extent that both Customer and Billtrust act as data controllers, Customer (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in **Exhibit A** to this Addendum, as applicable), which are incorporated by this reference and constitute part of this Addendum as follows:

i. Module One will apply;

ii. in Clause 7, the optional docking Clause will not apply;

iii. Clause 9, shall be deemed inapplicable;

iv. in Clause 11, the optional language will not apply;

v. In Clause 13, all square brackets removed, and all text therein is retained;

vi. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws that apply pursuant to Section 8.7 of the Terms;

vii. in Clause 18(b), disputes shall be resolved before the courts that are competent pursuant to Section 8.7 of the Terms;

viii. in Annex I:

- Part A: with the information set out in the heading and Exhibit A to this Addendum;
- Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and
- Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCCs;

ix. Annex II: with the Security Measures set out in Exhibit A to this Addendum

(d) **Module Two**: To the extent that Customer acts as data controller and Billtrust acts as data processor, Customer (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in Exhibit A to this Addendum, as applicable), which are incorporated by this reference and constitute part of this Addendum as follows:

i. Module Two will apply;

ii. in Clause 7, the optional docking Clause will not apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes shall be as set out in clause 4.3 of Module 2 of this Addendum;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws that apply pursuant to Section 8.7 of the Terms;

vi. in Clause 18(b), disputes shall be resolved before the courts that are competent pursuant to Section 8.7 of the Terms;

vii. in Annex I:

- Part A: with the information set out in the heading and Exhibit A to this Addendum;
- Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and
- Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCCs;

viii. Annex II: with the Security Measures set out in Exhibit A to this Addendum.

(e) **Module Three**: To the extent that Customer acts as Processor and Billtrust acts as Sub-Processor, Billtrust (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) and C (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained Exhibit A to this Addendum) as follows:

(i) Module Three will apply;

(ii) in Clause 7, the optional docking Clause will not apply;

(iii) in Clause 9, Option 1 Specific Authorisation applies;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 13, all square brackets removed, and all text therein is retained;

(vi) in Clause 17, Option 1 will apply, and the SCC's will be governed by the laws indicated under Section 16.8 of the Addendum;

(vii) in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 16.8 of the Addendum;

(viii) the certification of deletion of Personal Data described in Clause 8.5 of the SCCs shall be provided by the data importer to the data exporter only upon data exporter's written request.

(ix) the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.

(x) in Annex I:

- Part A: with the information set out in Exhibit A to this Addendum;
- Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and
- Part C: in accordance with the criteria set out in Clause 13(a) of the EU Standard Contractual Clauses;

(xi) Annex II: with the Minimum Security Measures of Exhibit B

**2. California**

2.1. **Definitions**:

i. For the purpose of interpreting the Addendum, the following terms shall have the meanings set out below:

a. "**Applicable Data Protection Laws**" includes the CCPA (as defined below) and the CCPA Regulations as may be amended from time to time.

b. "**CA Privacy Laws**" means, collectively, the California Consumer Privacy Act of 2018 (CCPA, codified at Civil Code section 1798.100 et seq.), the California Privacy Rights Act (CPRA), and all applicable regulations issued by the California Attorney General and/or the California Privacy Protection Agency implementing CCPA and CPRA.

ii. The terms "**Business Purpose**", "**Commercial Purpose**", "**Sale**", "**Sell**", along with their cognates whether capitalized or not, shall have the same meaning as in the CA Privacy Laws, and their related terms shall be construed accordingly.

iii. For the purpose of interpreting this Addendum, the following terms shall be interpreted as follows:

a. "**Contractor**" has the meaning given to it in Section 1798.140(j) of the California Civil Code.

b. "**Controller**" includes "**Business**" as defined under the CA Privacy Laws;

c. "**Data Subject**" includes "**Consumer**" as defined under the CA Privacy Laws;

d. "**Personal Data**" includes "**Personal Information**" as definedin Section 1798.140(o) of the California Civil Code;

e. "**Personal Data Breach**" includes "**Breach of the Security of the System**" as defined in Section 1798.8 of the California Civil Code;

f. "**Processor**" includes "**Service Provider**" in Section 1798.140(ag) of the California Civil Code;

2.2. Billtrust as a Service Provider or Contractor:

(a) Where Billtrust acts as a Data Processor or a sub-Processor on behalf of Customer in accordance with Section 3.1 of the Addendum:

i. Customer discloses Customer Personal Data to Billtrust solely for: (i) valid Business Purposes; and (ii) to enable Billtrust to perform the Processor Services under the Agreement(s).

ii. Billtrust shall not: (i) sell Personal Data; (ii) share personal data as defined in the CPRA; (iii) retain, use or disclose Customer Personal Data for any purpose other than providing the Processor Services specified in the Agreement(s) or as otherwise permitted by the CCPA and the CCPA Regulations. Billtrust certifies that it understands these restrictions and will comply with them.

iii. Billtrust shall permit the business to, upon notice of non-compliance with the CPRA, take reasonable and appropriate termination and suspension steps to stop and remediate unauthorized use of personal data.

**3. Canada**

3.1. **Definitions**:

(a) For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

i. "**Applicable Data Protection Laws**" includes PIPEDA (as defined below).

ii. "**Personal Data**" includes "**Personal Information**" as defined under PIPEDA (as defined below).

iii. "**Personal Data Breach**" includes "**Breach of Security Safeguards**" as defined under PIPEDA (as defined below).

iv. "**PIPEDA**" means the Federal Personal Information Protection and Electronic Documents Act.

v. **"Sub-Processor**" and "**Sub-processor**" include "**Third Party Organization**" as defined under PIPEDA.

3.2. **Necessary Consent.** Customer confirms that is has obtained a valid consent (as defined under PIPEDA), where necessary to Process Personal Data of each Data Subject.

**4. Switzerland**

4.1. **Definitions**:

(a) For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

i. "**Applicable Data Protection Laws**" includes the FADP (as defined below) and the OFADP (as defined below), as may be amended from time to time.

ii. "**Controller"** includes "Controller of the Data File" as defined under the FADP (as defined below).

iii. "**Data Subject**" includes the natural persons whose Personal Data is Processed.

iv. "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992.

v. "**OFADP**" means the Ordinance to the Federal Act on Data Protection ("OFADP")

vi. "**Personal Data**" includes "**Personal Data**" as defined under the FADP.

vii. "**Processing**" includes "**Processing**" as defined under the FADP.

viii. "**Swiss Restricted Transfer**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the FADP to a Third Country (as defined below) or an international organization.

ix. "**Third Country**" (as used in this Section) means a country outside of the EEA.

4.2. **Swiss Restricted Transfers.** With regard to any Swiss Restricted Transfer from Customer to Billtrust within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) the inclusion of the Third Country, a territory or one or more specified sectors within that Third Country, or the international organization in question to which Personal Data is to be transferred in the list published by the Swiss Federal Data Protection and Information Commissioner of States that provide an adequate level of protection for Personal Data within the meaning of the FADP;

(b) Billtrust's certification to any successor to the Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the FADP and the OFADP, as the case may be), provided that the Services are covered by the self-certification, if applicable;

(c) the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the FADP and the OFADP, as the case may be); or

(d) any other lawful basis, as laid down in FADP and the OFADP, as the case may be.

4.3. **Standard Contractual Clauses**:

(a) Customer (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in **Exhibit A** to this Addendum, as applicable), which are incorporated by this reference and constitute an integral part of this Addendum. The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in **Exhibit C** to this Addendum serves to supplement the Standard Contractual Clauses.

(b) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

(c) Where the Standard Contractual Clauses apply, Customer shall inform the Federal Data Protection and Information Commissioner about the use of the Standard Contractual Clauses before transferring the data outside the Swiss Confederation, when possible.

(d) The FDPIC shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP.

(e) The term "EU Member State" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with the SCCs.

(f) Until the new Federal Act on Data Protection of 25 September 2020 enters into force, and provided that the processing of personal data is governed by the Federal Act on Data Protection, the term 'personal data' also includes the data of legal entities.

**5. United Kingdom**

5.1. Definitions:

For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:

(a) "**Applicable Data Protection Laws**" includes the Data Protection Act 2018 and, when in full force and effect, the UK GDPR (as defined below).

(b) "**UK GDPR**" means the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

(c) "**UK Transfer Addendum**" means the template Addendum B.1.0 issued by the UK Information Commissioner's Office (ICO) and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the "Mandatory Clauses").

(d) "**UK Restricted Transfer**" includes any transfer of Personal Data (including data storage in foreign servers) subject to the UK GDPR to a third country outside of the UK or an international organization.

5.2. UK Restricted Transfers:

(a) With regard to any UK Restricted Transfer from Customer to Billtrust within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:

i. a valid adequacy decision pursuant to the requirements under the UK GDPR and the Data Protection Act 2018 that provides that the third country, a territory or one or more specified

sectors within that third country, or the international organization in question to which Personal Data is to be transferred ensures an adequate level of data protection;

ii. Service Provider's self-certifications to the E.U.-U.S. Privacy Shield Framework or any successor to the Privacy Shield Framework (only to the extent that such self-certification constitutes an "appropriate safeguard" pursuant to the UK GDPR and the Data Protection Act 2018, as the case may be), provided that the Services are covered by the self-certification, if applicable;

iii. the Standard Contractual Clauses (insofar as their use constitutes an "appropriate safeguard" under the UK GDPR and the Data Protection Act 2018); or

iv. any other lawful basis, as laid down in the UK GDPR and the Data Protection Act 2018, as the case may be.

5.3. Standard Contractual Clauses:

(a) Customer (which will take on the obligations of "data exporter" for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of "data importer" for the purposes of the Standard Contractual Clauses) hereby enter into, the Standard Contractual Clauses (including their additional constituent elements, as set out in **Exhibit A** to this Addendum, as applicable), which are incorporated by this reference and constitute an integral part of this Addendum. The Parties are deemed to have signed, accepted, and executed the Standard Contractual Clauses in their entirety, including the appendices as of the Effective Date. The text contained in **Exhibit C** to this Addendum serves to supplement the Standard Contractual Clauses.

(b) The parties hereby agree to incorporate the Standard Contractual Clauses which are amended and supplemented to the extent necessary by Exhibits A and C to this Addendum so that together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide standards of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

(c) In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

(d) PART 1 OF THE UK TRANSFER ADDENDUM. As permitted by Section 17 of the UK Transfer Addendum, the parties agree that:

i. Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed completed with the corresponding details set out in Exhibit A to this Addendum subject to the variations effected by the Mandatory Clauses described below; and

ii. Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled 'Data Importer' being deemed to have been ticked.

(e) PART 2 OF THE UK TRANSFER ADDENDUM. The Parties agree (i) to be bound by the Mandatory Clauses of the UK Transfer Addendum and (ii) In relation to any UK Restricted Transfer to which the UK Transfer Addendum applies, where the context permits and requires, any reference in this Addendum to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this section 5.3.

# EXHIBIT C: Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit C** (this "Exhibit"), the Parties provide additional safeguards to and additional redress to the Data Subjects to whom transferred Customer Personal Data pursuant to Standard Contractual Clauses relates. This Exhibit supplements and is made part of, but is not in variation or modification of, the Standard Contractual Clauses that may be applicable to the Restricted Transfer.

**1. Applicability of this Exhibit**

1.1. This Exhibit only applies with respect to Restricted Transfers when the Parties have concluded the Standard Contractual Clauses pursuant to the Addendum and its Exhibits.

**2. Definitions**

2.1. For the purpose of interpreting this Section, the following terms shall have the meanings set out below:

(a) "**Data Importer**" and "**Data Exporter**" shall have the same meaning assigned to them in the Standard Contractual Clauses concluded by the Parties.

(b) "**FISA**" means the U.S. Foreign Intelligence Surveillance Act.

(c) "**Schrems II Judgment**" means the judgment of the European Court of Justice in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.

2.2.

**3. Back doors**

3.1. Data Importer certifies that:

(a) it has not purposefully created back doors or similar programming that could be used to access Data Importer's Systems or Customer Personal Data subject to the Standard Contractual Clauses;

(b) it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and

(c) that national law or government policy does not require Data Importer to create or maintain back doors or to facilitate access to Personal Data or systems.

3.2. Data Exporter will be entitled to terminate the contract on short notice in those cases in which Data Importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform Data Exporter once their existence comes to its knowledge.

**4. Other Measures to Prevent Authorities from Accessing Personal Data**

4.1. Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement:

(a) Internal policies or procedures establishing that:

where Data Importer is prohibited by law from notifying the Data Exporter of an order from a public authority for transferred Personal Data, the Data Importer shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent Supervisory Authorities;

the Data Importer's legal team shall scrutinize requests for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid; and

if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request.

**5. Termination**

5.1. This Exhibit shall automatically terminate if the European Commission, a competent Member State Supervisory Authority, or an EEA or competent Member State court approves a different lawful transfer mechanism that would be applicable to the data transfers covered by the Standard Contractual Clauses (and if such mechanism applies only to some of the data transfers, this Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in this Addendum.