

## 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 Billtrust a corporation incorporated under the laws of the State of Delaware, and its relevant affiliates (“**Billtrust**”) and the customer agreeing to these terms (the “**Customer**”) (each, a “**Party**” and, collectively, the “**Parties**”). This Addendum forms part of the Agreement (as defined in Section 1 below) originally entered into between Customer and Billtrust. This Addendum replaces any data processing agreement that was previously concluded between the Customer and Billtrust.

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.

### 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 amend the Agreement to ensure that Personal Data (as defined below) transferred between the Parties is Processed in compliance with applicable data protection principles and legal requirements.

**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 the Billtrust Payments Network (BPN) Terms and Conditions or Billtrust Subscription Agreement and any of its predecessors, including the Billtrust Credit Master Services Agreement, signed by the Parties, as applicable;
  - (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) **“EEA Data Protection Laws”** means the GDPR and laws implementing or supplementing the GDPR;
- (d) **“Customer Personal Data”** means any Personal Data Processed by a Billtrust pursuant to or in connection with the Agreement(s), as applicable;
- (e) **“Controller Services”** means the Credit Subscription Services, the Business Payment Network, and the Business Directory under the Services Agreement, any other services for which Billtrust would factually act as a Controller, and Billtrust marketing activities as described under the Services Agreement;
- (f) **“Effective Date”** means the date the parties entered into the controlling Agreement, as defined in the Agreement;
- (g) **“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;
- (h) **“Personal Data Recipient”** means Billtrust, a Sub-processor, or both collectively;
- (i) **“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 **Exhibit B** hereto below;
- (j) **“Services”** means the services and other activities carried out by or on behalf of Billtrust for Customer pursuant to the Agreement.
- (k) **“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).
- (l) **“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;
- (m) **“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;
- (n) **“Supervisory Authority”** includes any competent authority tasked with the enforcement of the Applicable Data Protection Laws.

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 applicable, alone or jointly, 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. This Addendum will not apply to the Processing of Personal Data, where such Processing is not regulated by 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. Processor Services:**

- (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) When Billtrust acts as a Processor or a Sub-Processor in the context of this Addendum, the Processor Services Terms shall apply.

### **3.2. Controller Services:**

- (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) When Billtrust acts as a Controller in the context of this Addendum, the Controller Services Terms shall apply.

- 3.3. The Sections of the Addendum (including its exhibits) that are not mentioned in the above subsections 3.1 and 3.2 are applicable regardless of the role of the Parties, unless the 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 Section 3 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 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**, then the terms specified in **Exhibit B** with respect to the applicable jurisdiction(s) (“**Jurisdiction Specific Terms**”) shall apply in addition to the terms of this Addendum. 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 one of the jurisdictions listed in **Exhibit B**.
- (b) Billtrust may update **Exhibit B** 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 **Exhibit B** 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 **Exhibit B** within fourteen (14) days of receipt, Customer will be deemed to have consented to the updated **Exhibit B**.
- (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.
- (b) Billtrust may update **Exhibit C** from time to time to provide for additional safeguards to Personal Data subject to Restricted Transfers. Billtrust shall provide Customer prior written notice of any changes to Exhibit C by offering Customers a mechanism to subscribe to a notification system of updates as posted on the same page where the Exhibit C is posted. If Customer does not object to the updated **Exhibit C** within fourteen (14) days of the updates, Customer will be deemed to have consented to the updated **Exhibit C**.

## 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, where this Addendum is not in full force and effect.

## **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 Laws under this Addendum
- 8.3. 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.
- 8.4. In the event of any conflict between the Agreement (including any annexes and appendices thereto) and this Addendum, the provisions of this Addendum shall control, except where the applicable Jurisdiction Specific Terms will apply and take precedence as discussed in Section 6.1 (c) above.
- 8.5. 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.
- 8.6. 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), 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.
- 8.7. 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.

## **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.

## Controller to Controller Terms

### 1. Representations and Warranties

1.1. 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 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.

### 2. Controller Commitments

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

- (a) Processing is limited to that which is reasonably necessary to perform the Services under the applicable Agreement(s).
- (b) 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.
- (c) 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.
- (d) 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.

### 3. Sales of Personal Data

3.1. 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.

## Controller to Processor Terms

### 1. Processing Obligations

#### 1.1. Billtrust:

- (a) shall comply with all applicable laws in the Processing of Customer Personal Data, including Applicable Data Protection Laws;
- (b) shall 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;
- (c) shall only conduct transfers of Customer Personal Data in compliance with all applicable conditions, as laid down in Applicable Data Protection Laws;
- (d) shall 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
- (e) shall immediately inform Customer in the event that, in Billtrust's opinion, a Processing instruction given by Customer may infringe applicable laws.

#### 1.2. Customer:

- (a) shall 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.
- (b) Instructs Billtrust (and authorizes 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.
- (c) represents and warrants 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.

### 2. Billtrust Personnel

- 2.1. 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 fulfill the documented Processing instructions given to Billtrust by Customer or to comply with applicable laws.
- 2.2. 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.

### **3. Security of Processing**

- 3.1. 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.
- 3.2. In assessing the appropriate level of security, Billtrust shall take account, in particular, of the risks that are presented by the nature of such Processing activities, and particularly those related to possible Personal Data Breaches.
- 3.3. 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.
- 3.4. 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.

### **4. Use of Sub-Processors**

- 4.1. 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 9 and any possible further restrictions, as set out in the Agreement, as the case may be.
- 4.2. 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 in Section 9 of this Addendum. The list of Billtrust's Sub-processors is available at <https://www.billtrust.com/sub-processors/>.
- 4.3. 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 14 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.
- 4.4. With respect to each Sub-processor, Billtrust shall:
  - (a) 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 4.2; and
  - (b) impose terms between Billtrust and the prospective Sub-processor that:

- i. offer at least the same level of protection for Personal Data as those set out in this Addendum on the Sub-processor
- ii. meet the requirements of Applicable Data Protection Laws.

## **5. Rights of the Data Subjects**

5.1. 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.

5.2. With regard to the rights of the Data Subjects within the scope of this Section 5, Billtrust shall:

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

## **6. Personal Data Breach**

6.1. 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 sufficient information to allow Customer to meet any applicable obligations pursuant to the Applicable Data Protection Laws, such as to report to the Supervisory Authorities or any other competent authorities, or inform the Data Subjects of the Personal Data Breach.

6.2. 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.

6.3. 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.

## **7. Data Protection Impact Assessment and Prior Consultation**

7.1. 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 Client reasonably considers that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Laws but in each such case solely with regard to

Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the respective Personal Data Recipient.

## **8. Deletion or Return of Personal Data**

- 8.1. 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.
- 8.2. Billtrust shall promptly, following the date of cessation of Services involving the Processing of Customer Personal Data, at the choice of Customer delete or return all Personal Data to Customer as well as delete existing copies, unless Applicable Laws require storage of any such Personal Data.

## **9. Audit Rights**

- 9.1. 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 been 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/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), and 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 9 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.
- 9.2. Customer agrees to pay Billtrust, upon receipt of invoice, a reasonable fee based on the time spent, as well as to account for the materials expended, in relation to Customer exercising its rights under this Section 9 or the Standard Contractual Clauses 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, where applicable, as set out in **Exhibit B**.

**Exhibit A: Details of Processing**

Further details of the Processing, in addition to those described in the Agreement and this Addendum, include:

<b>The following details of processing apply to circumstances in which Billtrust is a Data Controller (and where the Standard Contractual Clauses that govern transfers between Data Controllers apply):</b>			
<b>Product</b>	<b>BPN</b>	<b>Credit</b>	<b>BBD</b>
<p><b>Data Subjects</b> The Personal Data transferred concerns the following categories of data subjects:</p>	Suppliers (current and prospective Billtrust customers).	Sole proprietors who are customers of Billtrust’s Customers.	Sole proprietors who are customers of Billtrust customers who are invoiced by a Billtrust customer
<p><b>Purposes of the transfer(s)</b> The transfer is made for the following purposes(s):</p>	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, and providing the Business Payment Network product to Billtrust Customers; to contact Billtrust customers, when required; to create a two-sided platform in which payable providers can deliver digital payments directly to the suppliers’ acceptance platforms.	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 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.
<p><b>Categories of data</b></p>	First and last name, email address, company	First and last name, business address, email address,	Company name (such as sole proprietor’s name), email address.

**The following details of processing apply to circumstances in which Billtrust is a Data Controller (and where the Standard Contractual Clauses that govern transfers between Data Controllers apply):**

Product	BPN	Credit	BBD
<p>The Personal Data transferred concerns the following categories of data:</p>	<p>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.</p>	<p>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; creditor 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.</p>	<p>Number of electronic payments, number of payments with paper checks, payment preferences (paper checks/electronic payment) (this is further aggregated).</p>
<p><b>Recipients</b> The Personal Data transferred may be disclosed to the following recipients or categories of recipients:</p>	<p>Payment gateways Service providers who provide:</p> <ul style="list-style-type: none"> <li>● cloud data storage services and SaaS-based integration platforms</li> <li>● co-location and infrastructure services</li> <li>● payment infrastructure platforms</li> <li>● ACH wire transaction facilitators</li> <li>● business intelligence software</li> <li>● big data analytics platform</li> </ul>	<p>Credit bureaus Credit analysts Factoring organizations Other Billtrust’s customers Service providers who provide:</p> <ul style="list-style-type: none"> <li>● hosting services</li> <li>● cloud data storage services and SaaS-based integration platforms</li> <li>● cloud-computing software</li> <li>● co-location and infrastructure services</li> <li>● electronic signature software</li> <li>● anti-money laundering solutions</li> <li>● payment infrastructure platforms</li> </ul>	<p>None.</p>

**The following details of processing apply to circumstances in which Billtrust is a Data Controller (and where the Standard Contractual Clauses that govern transfers between Data Controllers apply):**

Product	BPN	Credit	BBD
	<ul style="list-style-type: none"> <li>event logging platforms</li> </ul>	<ul style="list-style-type: none"> <li>ACH wire transaction facilitators</li> <li>business intelligence software</li> <li>big data analytics platform</li> <li>event logging platforms</li> <li>security solutions</li> <li>interactive voice response systems</li> </ul>	
<b>Sensitive data (if appropriate)</b> The Personal Data transferred concerns the following categories of sensitive data	N/A		
<b>Data protection registration information of the data exporter (where applicable)</b>	For Billtrust N/A For Customer: N/A		
<b>Contact points for data protection inquiries</b>	Billtrust: <a href="mailto:privacy@billtrust.com">privacy@billtrust.com</a> Customer: The contact point indicated in the Order Forms and/or SOWs pertaining to the Agreements.		

**The following details of processing apply to circumstances in which Billtrust is a Data Processor (and where the Controller to Processor SCCs apply):**

The subject matter of the Processing of Personal Data pertains to the provision of the Processor Services, as requested by the Customer.

The purpose of Processing of Personal Data pertains to the provision of specified products and services implementation under the Agreement(s).

The duration of the Processing of Personal Data is generally determined by Customer and is further subject to the terms of this Addendum and the Agreement(s), respectively, in the context of the contractual relationship between Billtrust and Customer.

The categories of Data Subjects to whom the Personal Data relates are customers of Customer.

The categories of Personal Data to be Processed identifiers, special categories of personal data, and commercial information. No special categories of Personal Data are processed.

The basic 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.

A description of technical and organizational security measures implemented by Billtrust is available in the **Exhibit A** in the Billtrust Subscription Agreement.

## 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, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.
  - 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. **“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 (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) 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.

## 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. **“CCPA”** means the California Consumer Privacy Act of 2018;
  - c. **“CCPA Regulations”** means the California Consumer Privacy Act Regulations;
- 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 CCPA, 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. **“Controller”** includes **“Business”** as defined under the CCPA;
  - b. **“Data Subject”** includes **“Consumer”** as defined under the CCPA;
  - c. **“Personal Data”** includes **“Personal Information”** as defined under the CCPA;
  - d. **“Personal Data Breach”** includes **“Breach of the Security of the System”** as defined in Section 1798.8 of the California Civil Code;
  - e. **“Processor”** includes **“Service Provider”** as defined under the CCPA;

### 2.2. Billtrust as a Service Provider:

- (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) 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.

### 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.

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.

## 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 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 (General Data Protection Regulation)” as has been amended, adopted, and forming part of the law of England, Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdraw) Act 2020.
- (c) “**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) 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.

## 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.

### 3. Applicability of Surveillance Laws to Data Importer and its Sub-processors

- 3.1. Billtrust (hereinafter, the “**Data Importer**”) represents and warrants that, as of the date of this Agreement(s), it has not received any national security orders of the type described in paragraphs 150-202 of the Schrems II judgment.
- 3.2. Data Importer represents that it does not expect to receive requests to disclose Customer Personal Data under FISA Section 702 because:
  - (a) Data Importer is not, (i) a telecommunications carrier, (ii) a provider of electronic communication service; (iii) a provider of processing services by means of an electronic communications system to the general public, given the nature of its business-to-business services; (iv) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; nor any other type of “electronic communications service provider” within the meaning of 50 U.S.C. § 1881(b)(4).“.
  - (b) If Data Importer were to be found eligible for FISA Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to UPSTREAM collection pursuant to FISA Section 702, as described in paragraphs 62 and 179 of the Schrems II judgment.
  - (c) Data Importer is not aware that companies operating in the same sector as Data Importer receive requests to disclose personal data.
4. Executive Order 12333 does not provide the U.S. government the ability to order or demand Data Importer to provide assistance for the bulk collection of information and Data Importer shall take no action pursuant to Executive Order 12333.

5. Data Importer commits to provide upon reasonable request information about the laws and regulations in the destination countries of the transferred Customer Personal Data applicable to Data Importer that would permit access by public authorities to the transferred Customer Personal Data, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data. The Data Importer providing the information referred to in this subparagraph 4 may choose the means to provide the information. Data Exporter agrees to cover the costs associated with this research.
6. Data Importer shall monitor any legal or policy developments that impact its inability to comply with its obligations under the Standard Contractual Clauses and this Exhibit, and promptly inform the Data Exporter of any such changes and developments. When possible, the Data Importer shall inform the Data Exporter of any such changes and developments ahead of their implementation.
7. **Obligations on the Data Importer Related to Orders for Compelled Disclosure of Customer Personal Data**
  - 7.1. In the event Data Importer receives an order from any third party for compelled disclosure of any personal data that has been transferred under the Standard Contractual Clauses, Data Importer shall:
    - (a) promptly notify the Data Exporter, unless prohibited under the law applicable to Data Importer, and, if prohibited from notifying the Data Exporter, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to the Data Exporter as soon as possible. This includes but it is not limited to informing the requesting public authority of the incompatibility of the order with the safeguards contained in Standard Contractual Clauses and the resulting conflict of obligations for Data Importer and documenting this communication;
    - (b) use reasonable lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable EEA Member State law or any other Applicable Data Protection Laws. Lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction. Data Exporter agrees to cover the costs of any associated legal actions;
    - (c) where possible, seek interim measures with a view to suspend the effects of the order until the competent court has decided on the merits;
    - (d) not disclose the requested Customer Personal Data until required to do so under the applicable procedural rules;
    - (e) provide the minimum amount of information permissible when responding to the request, based on a reasonable interpretation of the request.

## **8. Redirection of the Request to the Data Exporter**

- 8.1. Unless prohibited under the law applicable to the requesting third party, Data Importer shall use every reasonable effort to redirect the third party requesting the disclosure of any Customer Personal Data subject to the Standard Contractual Clauses that has been transferred to Data Importer to request data directly from Data Exporter.

## **9. Information on Requests of Access to Personal Data by Public Authorities**

- 9.1. Where allowed by law, Data Importer commits to provide Data Exporter with sufficiently detailed information on all requests of access to Personal Data by public authorities which the Data Importer has

received over a specified period of time (if any). Data Importer may choose the means to provide this information.

## **10. Back doors**

10.1. 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.

10.2. 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.

## **11. Information about Legal Prohibitions**

11.1. Data Importer will provide the Data Exporter information about the legal prohibitions on Data Importer to provide information under Sections 7 through 9 of this Exhibit above. Data Importer may choose the means to provide this information.

## **12. Other Measures to Prevent Authorities from Accessing Personal Data**

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

- (a) The technical, organizational, administrative, and physical measures described in **Exhibit A** of the Subscription Agreement entitled Security designed to protect the transferred Personal Data from unauthorized disclosure and access.
- (b) 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.

## **13. Termination**

13.1. 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.