

BILLTRUST DATA PROCESSING ADDENDUM

This Billtrust Data Processing Addendum, including all its exhibits (this “**Addendum**”), is entered into by and between Factor Systems, LLC d/b/a Billtrust acting on its own and as agent for the Billtrust Affiliates, as defined below (collectively referred to as “**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) between Billtrust or a Billtrust Affiliate and Customer. This Addendum replaces any data processing agreement or addendum 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 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 7.3. 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.

RECITALS

WHEREAS,

- A. the Parties entered into the Agreement and have retained the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement;
- B. 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;
- C. Customer, as a Data Controller (or, as applicable, a Data Processor), requires that its service providers who may Process Personal Data shared with them by Customer, take necessary measures to handle such information in compliance with Applicable Data Protection Laws; and
- D. 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, including but not limited to, as applicable, any Subscription Agreement, Master Services Agreement, services agreement, Statement of Work, Order Form, and any applicable documents incorporated by reference to any of the above.
 - b. “**Applicable Data Protection Laws**” means all laws that are applicable to the Processing of Personal Data under the Agreement, as further 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. Billtrust Affiliates specifically include, but are not limited to, as applicable, Anachron BV and iController BV.

- d. **“Customer Personal Data”** means any Personal Data Processed by Billtrust pursuant to or in connection with the Agreement(s), as applicable;
 - e. **“Controller Services”** means the Credit Subscription Services, the Business Payment Network (BPN), and the Billtrust Business Directory (BBD) (both as a freestanding Service, and as a component of BPN, as applicable), and any other services for which Billtrust would factually act as a Controller, and Billtrust marketing activities as described under the Agreement;
 - f. **“Documented Instructions”** means, with respect to Processor Services, the documented instructions of Customer, which Customer acknowledges are limited to those instructions that are documented in the Agreement and this Addendum as described herein.
 - g. **“EEA”** means the European Economic Area.
 - h. **“EEA Data Protection Laws”** means the GDPR and laws implementing or supplementing the GDPR;
 - i. **“Effective Date”** means the date the Parties entered into the controlling Agreement, as defined in the Agreement;
 - j. **“Exhibits”** means the annexures to current Addendum, respectively referred to as **“Exhibit A”** (SCC’s Appendices and Details of Processing), **“Exhibit B”** (Jurisdiction Specific Terms) or **“Exhibit C”** (Supplemental Clauses to the Standard Contractual Clauses), and which are included in this Addendum;
 - k. **“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;
 - l. **“Personal Data Recipient”** means Billtrust, a Sub-Processor, or both collectively;
 - m. **“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 in **Exhibit B**;
 - n. **“Services”** means the services and other activities carried out by or on behalf of Billtrust for Customer pursuant to the Agreement.
 - o. **“Standard Contractual Clauses”** or **“SCCs”** 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), 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.
 - p. **“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;
 - q. **“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;
 - r. **“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”**, and **“Processing”** and shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly. For the purposes of this Addendum and

its Exhibits, 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 and its Exhibits serve 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 (subject to the terms set forth below), 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:

- a. The terms of this Addendum shall be supplemented by Section 3.2 of this Addendum when:
 - In the context of this Addendum, 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; and
 - To the extent that, Billtrust acts as a Controller in the context of this Addendum.

3.2. Controller to Controller terms

- a. With respect to the Controller Services, each Party represents, warrants, and covenants that:
 - it is a Data Controller as to Personal Data with respect to the Processing of Personal Data under the Agreement, as applicable;
 - 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; and such Party will, upon request of the respective other Party, provide that other Party with copies of all Applicable Data Protection Laws or references to them (where relevant, and not including legal advice); and
 - 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.
- b. With respect to the Controller Services, each Party agrees that:
 - the Processing of Customer Personal Data for the purposes set out in the 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.
 - 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.
 - 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.
 - 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:

- a. The terms of this Addendum shall be supplemented by the section 3.4 of this Addendum when:

- In the context of this Addendum, with regard to the Processing of Personal Data in the context of the provision of the Processor Services:
 - when Customer acts as a Controller, Billtrust acts as a Processor; and
 - 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.
- 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:

- comply with all applicable laws in the Processing of Customer Personal Data, including Applicable Data Protection Laws;
- 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;
- without undue delay (or, where required by Applicable Data Protection Laws, immediately) inform Customer in the event that, in Billtrust's opinion, a Documented Instruction may infringe applicable laws.

b. The Customer:

- Shall provide all information which is applicable to the Customer, as provided in **Exhibit A** and keep all such information complete and up to date.
- 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.

c. New instruction/ New Privacy Compliance Requirements

- **New Instructions.** If Customer wants to issue additional instructions to Billtrust with respect to Processor Services, such instructions shall only become Documented Instructions to the extent they are mutually agreed to in an executed amendment to this Addendum or the Agreement. Customer acknowledges that any such additional instructions beyond those mutually agreed to in the Agreement or this Addendum may result in additional fees and charges to Customer.
- **New Privacy Compliance Requirements.** Each Party must notify the other Party if it reasonably determines that any new law or legal requirement prevents Billtrust from fulfilling its obligations under this Addendum or Applicable Data Protection Law, or otherwise materially alters its obligations hereunder. Each Party must also notify the other Party if it reasonably determines that any new law or legal requirement prevents Customer from fulfilling its obligations under this Addendum or Applicable Data Protection law, or otherwise materially alters its obligations hereunder. Any of the above situations shall be referred to as a "**New Privacy Compliance Requirement**".
- In the event of any New Privacy Compliance Requirement, the Parties shall use commercially reasonable efforts to come to a mutual agreement to identify a solution to address applicable compliance. In the event of any New Privacy Compliance Requirement that goes into legal effect, then either Party may in part or as a whole, as applicable, suspend the Processing of Personal Data by Billtrust, until such New Privacy Compliance Requirements are adequately addressed to the reasonable satisfaction of both Parties (provided, however, that notwithstanding any such suspension of Processing of Personal Data by Customer, Customer's payment obligations to Billtrust under the Agreement shall remain in place and in full force and effect during the full period of such suspension).
- In the event that the Parties cannot reach mutual agreement with respect to such New Privacy Compliance Requirement, then Customer may, at its option, exercise its right to terminate the Agreement pursuant to Section 9 of this Addendum below, and pay Billtrust the applicable termination fee referenced below. Any such

termination or failure to reach mutual agreement to adequately address such New Privacy Compliance Requirement shall not be considered to be a breach by either Party under this Addendum or the Agreement.

d. Billtrust Personnel

- 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 comply with the Documented Instructions or to comply with applicable laws.
- 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.

e. Security of Processing

- 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 (as more fully described in the "Security Requirements" of the Agreement) 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.
- 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.
- 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.

f. Use of Sub-Processors

- Customer provides general authorization to Billtrust to appoint (and permit each Sub-Processor appointed in accordance with this Section to appoint) Sub-Processors in accordance with this Section 3.4 and as otherwise set out in the Agreement, as the case may be.
- 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 this Section 3.4. The list of Billtrust's Sub-Processors is available at <https://www.billtrust.com/sub-processors/>. Customer may subscribe to any updates of Billtrust's Sub-processors using the RSS feed made available on the preceding weblink.
- Billtrust shall provide Customer with timely 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. More specifically, Billtrust will notify the Customer of such changes using the RSS feed that is made available on the above referenced Sub-Processor webpage. Customer acknowledges that the engagement of Sub-Processors is necessary for the performance of the Billtrust's obligations under this Agreement. 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. The notice must specify the grounds on which the objection is based.
- If Customer objects on reasonable grounds relating to data protection to the use of a new Sub-Processor, then Customer may suspend or terminate the affected Statement of Work in accordance with the termination provisions in Section 9 of this Addendum (but subject to any fees incurred by Customer prior to suspension or termination, and subject to the applicable termination fee language referenced below). Customer acknowledges and agrees that such termination right is Customer's sole and exclusive remedy for any Customer objection to any newSub-Processor.
- 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.

g. Rights of the Data Subjects

- It is the responsibility of Customer to respond to requests related to the rights of Data Subjects. 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 fulfillment 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. Billtrust reserves the right charge a reasonable fee for doing so.
- 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 Sub-Processors 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.

h. Personal Data Breach

- Billtrust shall notify Customer without undue delay upon Billtrust reasonably 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.
- 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.
- Billtrust's notification of or response to a Personal Data Breach under this Section 3.4 will not be construed as an acknowledgement by Billtrust of any fault or liability with respect to the Personal Data Breach.

i. Data Protection Impact Assessment and Prior Consultation

- Billtrust shall provide Customer with relevant information and documentation to the processing by Billtrust of Customer Personal Data (upon a written request and subject to obligations of confidentiality and Billtrust's reasonable security requirements and procedures), with regard to any data protection impact assessments, and prior consultations with supervisory authorities when the Customer reasonably determines 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. Billtrust reserves the right to charge a reasonable administrative fee for such assistance.

j. Deletion or Return of Personal Data

- 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.
- 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 or in the case Billtrust has a valid lawful basis for continuing to Process such Personal Data (including applicable record retention obligations). 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.

k. Audit Information

- Customer may request, and Billtrust will provide (subject to obligations of confidentiality and Billtrust's reasonable security requirements and procedures) relevant documentation, or any relevant audit report Billtrust

might have issued pursuant to the Agreement, to the extent that such information is of added value in demonstrating compliance with the Billtrust's obligations pursuant to current Section 3.4. 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 and the provisions hereof, other relevant information (excluding legal advice and commercially sensitive information (e.g. relating to pricing)) and/or documentation necessary to demonstrate compliance with this Section 3.4, and the obligations pursuant to the Applicable Data Protection Laws (Articles 32 to 36 of the GDPR in particular). The purpose of this information request is to confirm that Billtrust meets the requirement set out in Section 3.4 of the Addendum and the information request will be limited by that purpose.

- 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 and reasonably agreed to by Billtrust with regard to the Processing of the Personal Data by Billtrust, to the extent required by Applicable Data Protection Laws. The purpose of such audit is to confirm that Billtrust meets the requirements set out in Section 3.4 of the Addendum and the audit will be limited by that purpose. Billtrust shall provide the assistance described in this Section 3.4 (k) 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. In any event, on-site audits will be limited exclusively to Billtrust business facilities, and except to the extent specifically required by applicable law (and Customer provides Billtrust with reasonable documentary evidence of such specific requirement) under no circumstances whatsoever shall on-site audits be permitted with respect to data Processing facilities. Customer acknowledges and agrees that, without limitation, Billtrust may from time-to-time use service providers, including but not limited to cloud service providers, and other service providers with respect to the Services (such as, for example, Amazon Web Services and Microsoft Azure, among others), which Customer acknowledges routinely impose substantial limits on access to data Processing facilities, including with respect to audits. Billtrust shall have the right to reasonably adapt the scope of any on-site audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Billtrust customers' information. In addition, any audit shall be held in full compliance with Billtrust's security and confidentiality requirements and policies.
- Customer shall not conduct such audit more than once per year, unless required by applicable law or specific instruction of a competent data protection authority. Customer shall be solely responsible for any and all costs incurred by Customer with respect to this 3.4(k). Subject to applicable law, Billtrust reserves the right to charge additional fees to Customer related to any information and/or access provided pursuant to this Section 3.4(k).
- Any and all information provided or otherwise made available hereunder, as well as any results from an audit, shall constitute the exclusive Confidential Information of Billtrust, subject to the provisions on Confidential Information set out in the Agreement.

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. Customer understands and explicitly approves that Customer Personal Data may be Processed by Billtrust in a country outside the EEA, including but not limited to the United States of America. For the avoidance of doubt, this includes the right by Billtrust to store, display or access such Personal Data from or in any country in the world in which it is lawful to do so. Without limitation, Billtrust may conduct international data transfers between Billtrust Affiliates, and/or to Sub-Processors, for the purpose of data storage, and for implementing, configuring, providing, delivering, supporting,

maintaining and/or improving the Services, or for any other purpose authorized by the Agreement or this DPA. In relation to any transfers of Personal Data from the EEA to a non-EEA third country, Billtrust shall implement appropriate safeguards under Chapter V GDPR to ensure that the Personal Data is protected to a level equivalent to that required by the GDPR.

- 5.2. International transfers of Customer Personal Data within the scope of this Addendum shall be conducted in accordance with the applicable terms and conditions of **Exhibit B**.
- 5.3. 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**.
- 5.4. For avoidance of doubt, by entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses and **Exhibit B**, 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 Protection 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. 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 the **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 <https://www.billtrust.com/sub-processors/> 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. General Terms

- 7.1. 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 agreements or addenda entered into between Billtrust and Customer.
- 7.2. 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.
- 7.3. 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.

- 7.4. Should any provision of this Addendum or the Exhibits 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 and/ or the respective Exhibit will continue in effect.
- 7.5. 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.
- 7.6. 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.
- 7.7. This Addendum and its Exhibits are governed by the laws that apply to the Agreement. Any disputes between 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.

8. Data Protection Representative Representative(s)

- 8.1. 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/>

9. Termination

- 9.1. This Addendum 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 their nature, must survive termination of the Addendum.
- 9.2. In the event that Customer exercises an applicable right to terminate the Agreement or any applicable Order Form pursuant to any applicable provision of this Addendum, then such termination shall be subject to a termination fee in an amount equal to the greater of: (a) any applicable termination fee specified in the Agreement or any applicable Order Form; or (b) the average monthly fees paid or payable by Customer with respect to such Agreement or Order Form during the immediately preceding twelve (12) month period (the "**Termination Fee**"). Such Termination Fee shall be due and payable by Customer to Billtrust prior to the effective date of such termination. Any purported termination hereunder without payment of the applicable Termination Fee shall be null and void.

Preamble:

These Exhibits to the Billtrust Data Processing Addendum (“Addendum”) are incorporated into and made a part of the Agreement and the Addendum. Capitalized words not defined in the Exhibits shall have the meaning as set out in 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 the Agreement 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 Addendum with an address as set forth in the Agreement. Contact details: privacy@billtrust.com; see heading section of the 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 the 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 concerns the following categories of data subjects:	Customers (past, current and prospective) of Billtrust, also referred to as “Suppliers” Sole proprietors who are customers of Billtrust’s Customers staff of past, present and potential users of Billtrust Services.	Sole proprietors who are customers of Billtrust’s Customers.	Sole proprietors who are customers of Billtrust’s Customers

Processing Annex 1: Controller to Controller			
Product	BPN	Credit	BBD
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. 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.

Processing Annex 1: Controller to Controller			
Product	BPN	Credit	BBD
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 Service providers who provide: <ul style="list-style-type: none"> – cloud data storage services and SaaS-based integration platforms – co-location and infrastructure services – payment – infrastructure platforms – ACH wire – transaction facilitators – business intelligence software – big data analytics platform – event logging platforms 	Credit bureaus Credit analysts Factoring organizations Other Billtrust’s customers Service providers who provide: <ul style="list-style-type: none"> – hosting services – cloud data storage services and SaaS- based integration platforms – cloud-computing software – co-location and infrastructure services – electronic signature software – anti-money laundering solutions – payment – infrastructure platforms – ACH wire transaction facilitators – business intelligence software – big data analytics platform – event logging platforms – security solutions – interactive voice response systems 	Billtrust to Customer to deliver the Services pursuant to the Agreement.

Processing Annex 2: Controller to Processor and Processor to Processor	
Categories of data subjects whose personal data is transferred	Data Exporter's personnel Data Exporter's customers personnel 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. 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. 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.
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. Security Measures

Billtrust shall, during the Term of the Agreement, comply in all material respects with the security requirements set out in the Agreement.

D. List of Sub-Processors

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

E. Competent Supervisory Authority

The competent Supervisory Authority shall be determined as follows:

- 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.
- 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:**

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

- a. **“EEA”** means the European Economic Area.
- b. **“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.
- c. **“Supervisory Authority”** in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.
- d. **“Third Country”** (as used in this Section) means a country outside of the EEA.

1.2. Transfer Mechanisms:

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

- a. 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;
- b. 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;
- c. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard”
- d. under the GDPR, as the case may be); or
- e. 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 the Addendum serves to supplement the Standard Contractual Clauses. 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.
- b. **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**, as applicable), which are incorporated by this reference and constitute part of the Addendum as follows:
 - Module One will apply;
 - in Clause 7, the optional docking Clause will not apply;
 - Clause 9, shall be deemed inapplicable;
 - in Clause 11, the optional language will not apply;
 - In Clause 13, all square brackets removed, and all text therein is retained;
 - 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;

- in Clause 18(b), disputes shall be resolved before the courts that are competent pursuant to Section 8.7 of the Terms;
 - in Annex I:
 - Part A: with the information set out in the heading and Exhibit A;
 - Part B: with the relevant Processing Annex(ures) set out in Exhibit A; and
 - Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCCs;
 - Annex II: with the security measures set out in exhibit A to the Agreement
- c. **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**, as applicable), which are incorporated by this reference and constitute part of the Addendum as follows:
- Module Two will apply;
 - in Clause 7, the optional docking Clause will not apply; 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 the Addendum;
 - in Clause 11, the optional language will not apply;
 - 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;
 - in Clause 18(b), disputes shall be resolved before the courts that are competent pursuant to Section 8.7 of the Terms;
 - in Annex I:
 - Part A: with the information set out in the heading and **Exhibit A**;
 - Part B: with the relevant Processing Annex(ures) set out in **Exhibit A**; and
 - Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCCs;
 - Annex II: with the security measures set out in exhibit A to the Agreement.
- d. **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 Customer (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 the Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained in **Exhibit A**) as follows:
- Module Three will apply;
 - in Clause 7, the optional docking Clause will not apply;
 - in Clause 9, Option 1 Specific Authorisation applies;
 - in Clause 11, the optional language will not apply;
 - in Clause 13, all square brackets removed, and all text therein is retained;
 - 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;
 - in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 16.8 of the Addendum;
 - 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.
 - the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of the Addendum.
 - in Annex I:
 - Part A: with the information set out in **Exhibit A**;
 - Part B: with the relevant Processing Annex(ures) set out in **Exhibit A**; and
 - Part C: in accordance with the criteria set out in Clause 13(a) of the EU Standard Contractual Clauses;
 - Annex II: with the security measures of **Exhibit A** to the Agreement

2. California

2.1. Definitions:

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

- a. **“Applicable Data Protection Laws”** includes the CCPA (as defined below) and the CCPA
- b. Regulations as may be amended from time to time.
- c. **“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.

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.

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

- d. **“Contractor”** has the meaning given to it in Section 1798.140(j) of the California Civil Code.
- e. **“Controller”** includes **“Business”** as defined under the CA Privacy Laws;
- f. **“Data Subject”** includes **“Consumer”** as defined under the CA Privacy Laws;
- g. **“Personal Data”** includes **“Personal Information”** as defined in Section 1798.140(o) of the California Civil Code;
- h. **“Personal Data Breach”** includes **“Breach of the Security of the System”** as defined in Section 1798.8 of the California Civil Code;
- i. **“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 3.3 of the Addendum:
 - 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).
 - 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.
 - 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:

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

- a. **“Applicable Data Protection Laws”** includes PIPEDA (as defined below).
- b. **“Personal Data”** includes **“Personal Information”** as defined under PIPEDA (as defined below).
- c. **“Personal Data Breach”** includes **“Breach of Security Safeguards”** as defined under PIPEDA (as defined below).
- d. **“PIPEDA”** means the Federal Personal Information Protection and Electronic Documents Act.
- e. **“Sub-Processor”** and **“Sub-processor”** include **“Third Party Organization”** as defined under PIPEDA.

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

4. Switzerland

4.1. Definitions:

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

- a. **“Applicable Data Protection Laws”** includes the FADP (as defined below) and the OFADP (as defined below), as may be amended from time to time.
- b. **“Controller”** includes “Controller of the Data File” as defined under the FADP (as defined below).
- c. **“Data Subject”** includes the natural persons whose Personal Data is Processed.
- d. **“FADP”** means the Swiss Federal Act on Data Protection of 19 June 1992.
- e. **“OFADP”** means the Ordinance to the Federal Act on Data Protection (“OFADP”).
- f. **“Personal Data”** includes “Personal Data” as defined under the FADP.
- g. **“Processing”** includes “Processing” as defined under the FADP.
- h. **“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.
- i. **“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 the 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
- d. the FADP and the OFADP, as the case may be); or
- e. 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**, as applicable), which are incorporated by this reference and constitute an integral part of the 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** serves to supplement the Standard Contractual Clauses. 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.
- b. 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.

- c. The FDPIC shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the FADP.
- d. 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.
- e. 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 the Addendum and current Exhibit, 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:

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

- a. 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;
- b. 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;
- c. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under the UK GDPR and the Data Protection Act 2018); or
- d. 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**, as applicable), which are incorporated by this reference and constitute an integral part of the 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** 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 the 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:
 - 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 the Addendum subject to the variations effected by the Mandatory Clauses described below; and
 - 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 the 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.

A. Applicability of this Exhibit

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.

B. Definitions

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

“**Data Importer**” and “**Data Exporter**” shall have the same meaning assigned to them in the Standard Contractual Clauses concluded by the Parties.

C. Back doors

Data Importer certifies that:

- 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;
- it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and
- 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.

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.

D. Other Measures to Prevent Authorities from Accessing Personal Data

Notwithstanding the application of the security measures set forth in the Agreement, Data Importer will implement 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.

E. Termination

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, the Addendum will terminate only with respect to those transfers) and that does not require the additional safeguards set forth in the Addendum.