BILLTRUST

DATA PROCESSING ADDENDUM

# Service Providers

This Billtrust Data Processing Addendum (this “**Addendum**”), including its three appendices, is entered into by and between Factor Systems, LLC d/b/a Billtrust (“**Billtrust**”) and [SERVICE PROVIDER FULL LEGAL NAME] (the “**Service Provider**”) (each, a “**Party**” and, collectively, the “**Parties**”). This Addendum will become effective when the last Party signs it, as indicated by the date below that Party's signature (the “**Effective Date**”).

The Parties originally entered into the [MASTER SERVICE AGREEMENT NAME] (the “**Agreement**”) on [MONTH] [DAY], [YEAR]. 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**, Billtrust has certified its compliance with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework Principles (collectively, the “Privacy Shield Frameworks”) under which it is accountable for “Onward Transfer” of Personal Data received in reliance on the Privacy Shield Frameworks; and

**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**, 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:

## Definitions

* 1. Capitalized definitions not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified or supplemented below, the definitions of the Agreement shall remain in full force and effect.
  2. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:
     1. “**Applicable Laws**” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including laws of the European Union (or any member state thereof) and the laws of any other country, province, or state to which the Processing of the Personal Data is subject;
     2. “**Personal Data Recipient**” means Service Provider, a Sub- Processor, or both collectively;
     3. “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
     4. “**GDPR**” or “**General Data Protection Regulation**” 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,” as may be amended from time to time;
     5. “**Processor**” means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller;
     6. “**Processing**” (or any cognate terms) means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
     7. “**Personal Data**” means any information relating to an identified or identifiable\* natural person (a “**Data Subject**”) pertaining to Billtrust (and the Data Subjects, respectively) Processed by Service Provider on behalf of Billtrust pursuant to or in connection with the Agreement
        1. \*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
     8. “**Personal Data Breach**” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data which Service Provider Processes on behalf of Billtrust in connection with the Agreement;
     9. “**Service Provider**” means the party, as indicated in the opening paragraph of this Addendum, that has entered into the Agreement with Billtrust, including all affiliates of that entity that are also bound by the Agreement, if any;
     10. “**Services**” means the services and other activities carried out by or on behalf of Service Provider for Billtrust pursuant to the Agreement.
     11. **“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).
     12. Sub-Processor” means any third party appointed by or on behalf of Service Provider to Process Personal Data on behalf of Billtrust in connection with the Agreement;

## Applicability

* 1. 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.

## Processing of Personal Data

* 1. In the context of this Addendum and its appendices, with regard to the Processing of Personal Data, 1) when Billtrust acts as a Controller, Service Provider acts as a Processor; and 2) when Billtrust acts as a Processor, Service Provider acts as a sub-Processor. For the avoidance of doubt, both situations fall within the scope of and are covered by this Addendum.
  2. Service Provider warrants that it will:
     1. comply with all Applicable Laws in the Processing of Personal Data;
     2. Process Personal Data only on Billtrust’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 Service Provider, shall to the extent permitted by Applicable Laws, inform Billtrust of that legal requirement before the respective act of Processing of that Personal Data;
     3. only conduct transfers of Personal Data in compliance with all applicable conditions, as laid down in Applicable Laws; and
     4. promptly update, when necessary, all information, as provided in **Exhibit A**, attached hereto and incorporated by reference, and keep all such information complete and up to date.
  3. Billtrust instructs Service Provider (and authorizes Service Provider to instruct each Sub- Processor it engages) to Process Personal Data and, in particular, transfer Personal Data to any country or territory, only as reasonably necessary for the provision of the Services and consistent with the Agreement and this Addendum. In the event that, in Service Provider’s opinion, a Processing instruction given by Billtrust may infringe Applicable Laws, Service Provider shall immediately inform Billtrust.
  4. Service Provider represents and warrants that it is not, and has never been, subject to civil or criminal litigation, or government investigation, or consent decree, judgment, or order, regarding data privacy or information security, and that it has not suffered any material security breach or, if it has, that it has disclosed information regarding such security breach(es) to Billtrust.
  5. Where Billtrust is acting as a Processor, it warrants that it:
     1. Processes Personal Data only on behalf of its clients’ relevant documented instructions and, in turn, instructs Service Provider to carry out such Processing activities on behalf of Billtrust in accordance with said instructions of Billtrust’s clients; and
     2. has obtained the prior authorization from its respective immediate client, who is typically acting as a Controller regarding the processing of Personal Data, for subcontracting its activities to Service Provider and Sub- Processors.

## Service Provider Personnel

* 1. Service Provider shall take reasonable steps to ensure the reliability of any of its employees, agents, or contractors who may have access to Personal Data.
  2. Service Provider shall ensure that access to Personal Data is strictly limited to those individuals who need to know or access it, as strictly necessary to fulfill the documented Processing instructions given to Service Provider by Billtrust or to comply with Applicable Laws.
  3. Service Provider shall ensure that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.

## Security of Processing

* 1. Taking into account the state of the art and the high sensitivity of the Personal Data, Service Provider shall, with regard to Personal Data, implement and maintain [appropriate technical and organizational security measures](https://www.scheduleonce.com/trust/security) to ensure a level of security appropriate to that risk (including, as appropriate, the measures referred to in Article 32(1) of the GDPR) as well as assist Billtrust with regard to ensuring Billtrust’s compliance with its own obligations related to its security measures (including, without limitation, as required by Article 32 of the GDPR).
  2. In assessing the appropriate level of security, Service Provider 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.

## Subprocessing

* 1. Billtrust authorizes Service Provider to appoint (and permit each Sub-Processor appointed in accordance with this Section [6](#_Ref472956474) to appoint) Sub- Processors in accordance with this Section [6](#_Ref472956474) and any possible further restrictions, as set out in the Agreement, as the case may be.
  2. Service Provider may continue to use those Sub-Processors already engaged by Service Provider as of the date of this Addendum, subject to Service Provider meeting the obligations set out in Section 6.5. The list of Service Provider’s Sub- Processors as of the Effective Date is provided in **Exhibit B**.
  3. Service Provider shall provide Billtrust prior written notice of the appointment of any new Sub-Processor by email to [privacy@billtrust.com](mailto:ComplianceDept@billtrust.com) including full details of the Processing to be undertaken by that respective Sub- Processor.
  4. If Billtrust does not explicitly notify Service Provider in writing of any objections to the proposed appointment within 14 days of the receipt of such notice, Billtrust shall be deemed to have consented to the proposed appointment. If Billtrust objects to a proposed appointment, the Parties will, for a period of no more than 30 days from the date of Billtrust’s refusal, work together in good faith to attempt to find a commercially reasonable solution for Billtrust that avoids the use of the objected-to Sub- Processor.
  5. With respect to each Sub- Processor, Service Provider shall:
     1. before the Sub- Processor first Processes Personal Data (or, where relevant, in accordance with Section [6.2](#_Ref472933585)), 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; and must disclose the result of the conducted due diligence procedure to Billtrust and provide Billtrust with the documents used in the due diligence procedure upon request of Billtrust; and
     2. ensure that the arrangement between Service Provider and the prospective Sub- Processor is governed by a written contract that includes terms which offer at least the same level of protection for Personal Data as those set out in this Addendum, and that such terms meet the requirements of Applicable Laws.
  6. Where any Sub- Processor fails to fulfill its data protection obligations under such written contract (or in the absence thereof, as the case may be), Service Provider shall remain fully liable to Billtrust for the performance of the respective Sub- Processors’ obligations under such contract.

## Rights of the Data Subjects

* 1. Taking into account the nature of the Processing, Service Provider shall assist Billtrust by implementing appropriate technical and organizational measures, insofar as this is possible, to respond to requests to exercise rights of the Data Subjects under Applicable Laws.
  2. With regard to the rights of the Data Subjects within the scope of this Section 7, Service Provider shall:
     1. promptly notify Billtrust if any Personal Data Recipient receives a request from a Data Subject under any Applicable Law with respect to Personal Data;
     2. ensure that the Personal Data Recipient does not respond to that request, except on the documented instructions of Billtrust, or as required by Applicable Laws to which the Personal Data Recipient is subject, in which case Service Provider shall, to the extent permitted by Applicable Laws, inform Billtrust of that legal requirement before the Personal Data Recipient responds to the request; and
     3. promptly comply with any documented instructions from Billtrust regarding response to a request to exercise rights of the Data Subjects under Applicable Laws.

## Personal Data Breach

* 1. If Service Provider discovers, is notified of, or has reason to suspect a Personal Data Breach affecting Personal Data, Service Provider will provide notice to Billtrust within 24 hours of becoming aware of a confirmed or suspected Personal Data Breach.
  2. Service Provider shall provide Billtrust with sufficient information to assist Billtrust, or to allow Billtrust to assist its clients, so that each affected entity can meet its respective obligations pursuant to Applicable Laws, including any obligations to report the Personal Data Breach to the competent supervisory authorities, and/or inform the Data Subjects.
  3. Service Provider shall co-operate with Billtrust and take all reasonable commercial steps (at Service Provider’s own expense) to assist Billtrust in the investigation, mitigation, and remediation of each such Personal Data Breach.
  4. [Intentionally Omitted]

## Data Protection Impact Assessment and Prior Consultation

* 1. Service Provider shall provide Billtrust with relevant information and documentation, and assist Billtrust in complying with its obligations, with regard to any data protection impact assessments or prior consultations with supervisory authorities, when Billtrust determines that such data protection impact assessments or prior consultations are required pursuant to Applicable Laws (including, without limitation, Article 35 or 36 of the GDPR), but in each such case solely with regard to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the respective Personal Data Recipient.

## Deletion or Return of Personal Data

* 1. Service Provider shall provide Billtrust with the technical means, consistent with the way the Services are provided, to request the deletion of Personal Data upon the request of Billtrust, unless Applicable Laws require storage of any such Personal Data.
  2. Service Provider shall promptly, following the date of cessation of Services involving the Processing of Personal Data, at the choice of Billtrust, delete or return all Personal Data to Billtrust, as well as delete existing copies, unless Applicable Laws require storage of any such Personal Data. In the event that Billtrust has not specified its choice, it shall be deemed that Service Provider is obliged to delete all Personal Data from Billtrust.
  3. Service Provider shall also cause all Sub- Processors that may have received any Personal Data to delete or return, as applicable, all such Personal Data without undue delay.

## Audit Rights

* 1. Billtrust may request, and Service Provider will provide (subject to obligations of confidentiality), a current SOC 2 audit report, ISO 27001 certificate, or other substantially similar audit report.
  2. If Billtrust after having reviewed such audit report(s), still deems that it requires additional information (for example, Service Provider’s policies and procedures regarding data protection, information from Service Provider’s Sub- Processors, or any other relevant information) Service Provider shall further assist and make available to Billtrust all such additional information and/or documentation (including relevant provisions of contracts with Sub- Processors) necessary to demonstrate compliance with this Addendum and/or Applicable Laws.
  3. In addition, Service Provider shall allow for and contribute to audits, including remote inspections of the Services, by Billtrust (on behalf of itself or its clients) or an auditor mandated by Billtrust (on behalf of itself or its clients) with regard to the Processing of the Personal Data by the Personal Data Recipient.

1. **Jurisdiction Specific Terms**
   1. To the extent Service Provider processes Personal Data originating from, or protected by, Applicable Laws in one of the jurisdictions listed in **Exhibit C**, then the terms specified in **Exhibit C** with respect to the applicable jurisdiction(s) (“Jurisdiction Specific Terms”) shall apply in addition to the terms of this Addendum.
   2. Billtrust may update **Exhibit C** from time to time, to reflect changes in or additions to Applicable Laws to which Billtrust is subject. If Billtrust updates **Exhibit C**, it will provide the updated **Exhibit C** to Service Provider. If Service Provider does not object to the updated **Exhibit C** within 14 days of receipt, Service Provider will be deemed to have consented to the updated **Exhibit C**.
   3. 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 take precedence.
2. **No Selling of Personal Data**
   1. Service Provider acknowledges and confirms that it does not receive any Personal Data as consideration for any services or other items that Service Provider provides to Billtrust. Billtrust retains all rights and interests in Personal Data. Service Provider agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Service Provider to qualify as selling Personal Data under Applicable Laws.
3. **Liability**
   1. Service Provider shall be fully liable to Billtrust for any breach of the Agreement and this Addendum, and the obligations set out therein (including by means of additional contract, as the case may be), by any Personal Data Recipient, without prejudice to the liability of Service Provider in accordance with Applicable Laws.

## Indemnification

* 1. [Intentionally Omitted]

## General Terms

* 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 Service Provider and Billtrust.
  2. All clauses of the Agreement, that are not explicitly amended or supplemented by the clauses of this Addendum, and as long as this does not contradict with compulsory requirements of Applicable Laws under this Addendum, remain in full force and effect and shall apply.
  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 control.
  4. Should any provision of this Addendum be found legally invalid or unenforceable, then the invalid or unenforceable provision will be deemed superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of the Addendum will continue in effect.
  5. If Service Provider makes a determination that it can no longer meet any of its obligations in accordance with this Addendum, it shall promptly notify Billtrust of that determination, and cease the Processing or take other reasonable and appropriate steps to remediate.
  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. In the event that Service Provider materially breaches this Addendum, or suffers a material Personal Data Breach, Billtrust may, upon written notice to the Service Provider, terminate the relevant Service Agreement immediately (or upon such date as Billtrust selects), with no further fees due, other than what has been accrued up to and including the date of termination.

# Exhibit A: Details of Processing

I. Categories of data, categories of data subjects and purposes of the Processing

* 1. Categories of Personal Data

The Personal Data being Processed by Processor may concern the following categories of data:

* With respect to personnel of the Billtrust, personal details, including information that identifies the data subject such as name, employer, address, e-mail, telephone number, location and other contact details. With respect to customers of Billtrust, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.
  1. Categories of data subjects

The Personal Data Processed by Processor may concern the following categories of data subjects:

* Employees, suppliers, contractors, agents, directors, officers, customers, members, and/or partners of the Controller and/or its affiliates
  1. Purpose and nature of the Processing operations

Personal Data may be Processed by Processor for the following purposes:

* All processing operations required to facilitate provision of software and services to the Controller in accordance with the Agreement.

as further described in Processor’s audit reports and IT security policy.

* 1. Special categories of data

None.

# Exhibit B: Jurisdiction-Specific Terms

## Transfers of EEA Personal Data

* 1. Definitions:
     1. For the purpose of interpreting the Addendum, the following terms shall have the meanings set out below:
        1. “**EEA**” means the European Economic Area, consisting of the EU Member States, and Iceland, Liechtenstein, and Norway.
        2. “**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.
        3. “**Third Country**” (as used in this Section) means a country outside of the EEA.
  2. Transfer Mechanisms:
     1. 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:
        1. 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;
        2. 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;
        3. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under the GDPR, as the case may be); or
        4. any other lawful basis, as laid down in the GDPR, as the case may be.
  3. Standard Contractual Clauses:
     1. 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.
     2. 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.

## California

* 1. Definitions:
     1. For the purpose of interpreting the Addendum, the following terms shall have the meanings set out below:
        1. “**Applicable Data Protection Laws**” includes the CCPA (as defined below) and the CCPA Regulations as may be amended from time to time.
        2. “**CCPA**” means the California Consumer Privacy Act of 2018;
        3. “**CCPA Regulations**” means the California Consumer Privacy Act Regulations;
     2. 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.
     3. For the purpose of interpreting this Addendum, the following terms shall be interpreted as follows:
        1. “**Controller**” includes “**Business**” as defined under the CCPA;
        2. “**Data Subject**” includes “**Consumer**” as defined under the CCPA;
        3. “**Personal Data**” includes “**Personal Information**” as defined under the CCPA;
        4. “**Personal Data Breach**” includes “**Breach of the Security of the System**” as defined in Section 1798.8 of the California Civil Code;
        5. “**Processor**” includes “**Service Provider**” as defined under the CCPA;
  2. Billtrust as a Service Provider:
     1. Where Billtrust acts as a Data Processor or a sub-Processor on behalf of Customer in accordance with Section 3.1 of the Addendum:
        1. 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).
        2. 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.

## Canada

* 1. **Definitions**.:
     1. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:
        1. “**Applicable Data Protection Laws**” includes PIPEDA (as defined below).
        2. “**Personal Data**” includes “**Personal Information**” as defined under PIPEDA (as defined below).
        3. “**Personal Data Breach**” includes “**Breach of Security Safeguards**” as defined under PIPEDA (as defined below).
        4. "**PIPEDA**" means the Federal Personal Information Protection and Electronic Documents Act.
        5. **“Sub-Processor**” and “**Sub-processor**” include “**Third Party Organization**” as defined under PIPEDA.
  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.

## Switzerland

* 1. Definitions:
     1. For the purpose of interpreting this Addendum, the following terms shall have the meanings set out below:
        1. “**Applicable Data Protection Laws**” includes the FADP (as defined below) and the OFADP (as defined below), as may be amended from time to time.
        2. “**Controller”** includes “Controller of the Data File” as defined under the FADP (as defined below).
        3. “**Data Subject**” includes the natural persons whose Personal Data is Processed.
        4. “**FADP**” means the Swiss Federal Act on Data Protection of 19 June 1992.
        5. “**OFADP**” means the Ordinance to the Federal Act on Data Protection (“OFADP”)
        6. “**Personal Data**” includes “**Personal Data**” as defined under the FADP.
        7. “**Processing**” includes “**Processing**” as defined under the FADP.
        8. “**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.
  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:
     1. 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;
     2. 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;
     3. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under the FADP and the OFADP, as the case may be); or
     4. any other lawful basis, as laid down in FADP and the OFADP, as the case may be.
  3. Standard Contractual Clauses:
     1. 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 appendicesas of the Effective Date. The text contained in **Exhibit C** to this Addendum serves to supplement the Standard Contractual Clauses.
     2. 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.
     3. 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.

## United Kingdom

* 1. Definitions:

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

* + 1. “**Applicable Data Protection Laws**” includes the Data Protection Act 2018 and, when in full force and effect, the UK GDPR (as defined below).
    2. “**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.
    3. “**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.
  1. UK Restricted Transfers:
     1. 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:
        1. 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;
        2. 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;
        3. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under the UK GDPR and the Data Protection Act 2018); or
        4. any other lawful basis, as laid down in the UK GDPR and the Data Protection Act 2018, as the case may be.
  2. Standard Contractual Clauses:
     1. 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.

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. 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**
   1. For the purpose of interpreting this Section, the following terms shall have the meanings set out below:
      1. “**Data Importer**” and “**Data Exporter**” shall have the same meaning assigned to them in the Standard Contractual Clauses concluded by the Parties.
      2. “**FISA**” means the U.S. Foreign Intelligence Surveillance Act.
      3. “**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**
   1. Service Provider (hereinafter, the “**Data Importer**”) represents and warrants that, as of the Effective 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.
   2. Data Importer represents that it does not expect to receive requests to disclose Customer Personal Data under FISA Section 702 because:
   3. 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).“.
   4. 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.
   5. 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**
   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:
      1. 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;
      2. 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;
      3. where possible, seek interim measures with a view to suspend the effects of the order until the competent court has decided on the merits;
      4. not disclose the requested Customer Personal Data until required to do so under the applicable procedural rules;
      5. 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**
   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**
   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**
    1. Data Importer certifies that:
       1. 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;
       2. it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and
       3. 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.
    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**
    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**
    1. Notwithstanding the application of the security measures set forth in the Addendum, Data Importer will implement:
       1. 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.
       2. 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.

1. **Termination**
   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.

**[ THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK ]**

**[ SIGNATURE PAGE TO THE BILLTRUST DATA PROCESSING ADDENDUM FOLLOWS ]**

Each Party is signing this Addendum on the date stated below that Party’s signature.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Factor Systems, LLC dba Billtrust** | |  | [Service Provider Legal Company Name] (Service Provider) | |
|  | |  |  | |
| Signature | |  | Signature | |
|  | |  |  | |
| Name | |  | Name | |
|  | |  |  | |
| Title | |  | Title | |
|  | |  |  | |
| Date | |  | Date | |
|  |  | | |
|  |  | | |

**[ SIGNATURE PAGE TO THE BILLTRUST DATA PROCESSING ADDENDUM ]**

Exhibit A

1. Further details of the Processing, in addition to the ones laid down in the Agreement and this Addendum, include:
   1. The subject matter of the Processing of Personal Data is:
      1. The subject matter of the Processing of Personal Data pertains to the provision of Services, as requested by Billtrust.
   2. The duration of the Processing of Personal Data is:
      1. The duration of the Processing of Personal Data is generally determined by Billtrust and is further subject to the terms of this Addendum and the Agreement, respectively, in the context of the contractual relationship between Billtrust and Service Provider.
   3. The nature and purpose of the Processing of Personal Data is:
      1. The purpose of Processing of Personal Data pertains to the provision of payment orchestration Services under the Agreement.
   4. The categories of Personal Data to be Processed are:
      1. With respect to personnel of the Billtrust, personal details, including information that identifies the data subject such as name, employer, address, e-mail, telephone number, location and other contact details. With respect to customers of Billtrust, name, address, e-mail, telephone number, location, and billing and payment details such as bank account and credit or debit card numbers.
   5. The categories of Data Subjects to whom the Personal Data relates are:
      1. Personnel and customers of Billtrust
   6. Description of the technical and organisational security measures implemented by Service Provider:
      1. As provided in Schedule C of the Agreement
   7. The identity and contact information of the Data Protection Officer of Service Provider (if applicable) is:
      1. As provided in Schedule C of the Agreement
   8. The identity and contact information of the EU representative of Service Provider (if applicable) is:
      1. [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_]

Exhibit B

**List of Sub- Processors**

Below is a list of the Sub- Processors of Service Provider as at the Effective Date of the Addendum:

|  |  |  |
| --- | --- | --- |
| **Subprocessor** | **Purpose** | **Location** |
| Auth0 | Spreedly direct customer portal login | USA |
| AWS | Cloud data processing | USA |
| FiveTran | SaaS data integration service | USA |
| FIS/Global/Vantiv | Account updater service | UK |
| Looker | Business intelligence and visualization for analytics | USA |
| Slack | Private customer communication | USA |
| Snowflake | Data warehousing | USA |
| Zendesk | Inbound customer support and help center/community | USA |

Exhibit C

**Jurisdiction Specific Terms**

1. **Transfers of EU Personal Data**
   1. “**Restricted Transfer of EU Personal Data**” (as used in this Section) means any transfer of Personal Data (including data storage on foreign servers) that would be prohibited by the GDPR in the absence of the execution of the Standard Contractual Clauses (as defined below) or another lawful data transfer mechanism;
   2. “**Standard Contractual Clauses**” (as used in this Section) means the contractual clauses adopted by Decision of the European Commission (Commission Decision C(2010)593) for the purpose of adducing adequate protection of Personal Data transferred from a Controller to a Processor established in a third country, where the legislation in such third country has not been deemed to provide an adequate level of data protection.
   3. With regard to any Restricted Transfer of EU Personal Data from Billtrust to Service Provider within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:
      1. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under Article 46 of the GDPR); or
      2. any other lawful basis, as laid down in the GDPR, as the case may be.
   4. This Addendum hereby incorporates by reference the Standard Contractual Clauses (updated from time to time to reflect the latest version promulgated by the European Commission) for Billtrust (as “data exporter”) to Service Provider (as “data importer”) transfers, where Appendices 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum. The Parties are deemed to have accepted, executed, and signed the Standard Contractual Clauses where necessary, in their entirety (including the Appendices thereto, and including the “Illustrative Indemnification Clause” as an operative clause).
   5. 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 control.
2. **California**
   1. “**Applicable Laws**” (as used in the Addendum) includes the California Consumer Privacy Act of 2018, Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018 (“**CCPA**”) as may be amended from time to time.
   2. “**Business Purpose**” (as used in this Section) shall have the same meaning as in the CCPA;
   3. “**Commercial Purpose**” (as used in this Section) shall have the same meaning as in the CCPA;
   4. “**Controller**” (as used in the Addendum) includes “**Business**” as defined under the CCPA.
   5. “**Data Subject**” (as used in the Addendum) includes “**Consumer**” as defined under the CCPA.
   6. “**Personal Data**” (as used in the Addendum) includes “**Personal Information**” as defined under the CCPA.
   7. “**Personal Data Breach**” (as used in the Addendum) includes “**Breach of the Security of the System**” as defined under the CCPA.
   8. “**Processor**” (as used in the Addendum) includes “**Service Provider**” as defined under the CCPA.
   9. Billtrust discloses Personal Data to Service Provider solely for: (i) valid Business Purposes; and (ii) to enable Service Provider to perform the Services.
   10. Service Provider shall not: (i) sell Personal Data; (ii) retain, use or disclose Personal Data for a Commercial Purpose other than providing the Services specified in the Agreement or as otherwise permitted by the CCPA; nor (iii) retain, use, or disclose Personal Data except where permitted under the Agreement between Billtrust and Service Provider. Service Provider certifies that it understands these restrictions and will comply with them.
3. **United Kingdom**
   1. “**Applicable Laws**” (as used in the Addendum) includes the Data Protection Act 2018.