BILLTRUST

DATA PROCESSING ADDENDUM

# VENDORS

This Billtrust Data Processing Addendum (this “**Addendum**”), including its exhibits, is entered into by and between Factor Systems, LLC d/b/a Billtrust, acting on its own and as agent for the Billtrust Affiliates (collectively referred to as “**Billtrust**”), and Spreedly, Inc. (the “**Vendor**”) (each, a “**Party**” and, collectively, the “**Parties**”). This Addendum (including its exhibits) form part of any written or electronic agreement(s) between Billtrust or a Billtrust Affiliate and Vendor or a Vendor affiliate for the purchase of services pursuant to which the Vendor or a Vendor affiliate processes Personal Data for which Billtrust or a Billtrust Affiliate qualifies as a Controller or Processor (the **“Agreement”**).

This Addendum sets out obligations of the Parties with respect to data protection in relation to the Agreement. The Addendum will become effective when the last Party signs it, as indicated by the date below that Party's signature (the “**Effective Date**”). For the purposes of this Addendum only, and except where indicated otherwise, the term “Vendor” shall include Vendor and Vendor affiliates and the term “Billtrust” shall include Billtrust and/or where applicable Billtrust Affiliates.

To the extent of any conflict or inconsistency between the provisions of this Addendum 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. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended or supplemented by, and including, this Addendum and its exhibits.

**RECITALS**

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

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

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

1. **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 Data Protection 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. “**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.
        3. “**Billtrust Personal Data**” means any Personal Data Processed by or on behalf of Vendor on behalf of Billtrust and/or any Billtrust Affiliate pursuant to or in connection with the Agreement. This definition is used when Billtrust acts as a Controller and may include Billtrust human resources data, business contact information, and/or vendor relationship data, among other data types.
        4. “**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;
        5. “**Customer**” means a natural person or entity that receives products or services from Billtrust and/or any of Billtrust Affiliates.
        6. “**Customer Personal Data**” means any Personal Data originating from the Customer and Processed by or on behalf of Vendor, on behalf of Billtrust and/or any Billtrust Affiliate pursuant to or in connection with the Agreement. This definition is used when Billtrust acts as a Processor.
        7. “**GDPR**” or “**General Data Protection Regulation**” means, as appropriate and as amended from time to time, 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,”;
        8. “**Processor**” means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller;
        9. “**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;
        10. “**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 Vendor on behalf of Billtrust pursuant to or in connection with the Agreement

\**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*;

* + - 1. “**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 Vendor Processes on behalf of Billtrust and/ or in connection with the Agreement;
      2. “**Personal Data Recipient**” means Vendor, a Sub-Processor, or both collectively;
      3. “**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);
      4. “**Vendor**” 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;
      5. “**Services**” means the services and other activities carried out by or on behalf of Vendor for Billtrust and/or any Billtrust Affiliate pursuant to the Agreement;
      6. **“Standard Contractual Clauses”** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914 (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);
      7. "**Sub-Processor**” means any third party appointed by or on behalf of Vendor to Process Personal Data on behalf of Billtrust in connection with the Agreement;
      8. “**Supervisory Authority**” in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR; in the context of the UK GDPR, means the UK Information Commissioner’s Office; and in the context of the FADP, the FDPIC. (see definitions in **Exhibit D**)

1. **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.
2. **Processing of Personal Data**
   1. In the context of this Addendum and its exhibits, with regard to the Processing of Personal Data, 1) Billtrust may act as a Controller, and Vendor may act as a Processor; or 2) Billtrust may act as a Processor, and Vendor may act as a Sub-Processor. For the avoidance of doubt, the aforementioned situations fall within the scope of and are covered by this Addendum. The respective roles of the Parties for the Processing of Personal Data in the context of the Agreement is set out in **Exhibit A (Details of processing)**, Section A.
      * 1. The Parties acknowledge and agree that in relation to any Billtrust Personal Data provided or made available to Vendor for Processing in connection with the Services, Billtrust is the Controller and Vendor is a Processor, depending on the Services described in the relevant Agreement;
        2. in relation to any Customer Personal Data, Customer is the Controller, Billtrust is a Processor, and Vendor is a Sub-Processor.
   2. Vendor warrants:
      * 1. to comply with all Applicable Data Protection Laws in the Processing of Personal Data; and

***When Vendor is acting as a Processor or Sub-Processor:***

* + - 1. Process Personal Data pursuant to the Agreement (including with regard to international transfers of Personal Data), unless such Processing is required by Applicable Data Protection Laws to which the relevant Personal Data Recipient is subject, in which case Vendor, shall to the extent permitted by Applicable Data Protection Laws, inform Billtrust of that legal requirement before the respective act of Processing of that Personal Data;
      2. only conduct transfers of Personal Data in compliance with all applicable conditions, as laid down in Applicable Data Protection Laws; and
      3. promptly update, when necessary, all information, as provided in **Exhibit A (Details of processing)**, attached hereto and incorporated by reference, and keep all such information complete and up to date.
  1. Where Vendor is acting as a Processor or Sub-Processor, Billtrust instructs Vendor (and authorizes Vendor to instruct each Processor or 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, this Addendum and the relevant Exhibits. In the event that, in Vendor’s opinion, a Processing instruction given by Billtrust may infringe Applicable Data Protection Laws, Vendor shall immediately inform Billtrust.
  2. **Exhibit A** sets forth certain information regarding Vendor’s Processing of Personal Data. The Parties may from time to time amend Exhibit A by mutual agreement.
  3. Where Billtrust is acting as a Processor, it warrants that it:
     + 1. Processes Personal Data only on behalf of its Customers’ relevant documented instructions and, in turn, instructs Vendor to carry out such Processing activities on behalf of Billtrust in accordance with said instructions of Billtrust’s Customers; and
       2. has obtained the prior authorization from its respective immediate Customer, who is typically acting as a Controller regarding the processing of Personal Data, for subcontracting its activities to Vendor.

1. **Vendor Personnel**
   1. Vendor shall take reasonable steps to ensure the reliability of any of its employees, agents, or contractors who may have access to Personal Data.
   2. Vendor 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 Vendor by Billtrust or to comply with Applicable Data Protection Laws.
   3. Vendor shall ensure that all such individuals are subject to formal confidentiality undertakings, professional obligations of confidentiality, or statutory obligations of confidentiality.
2. **Security of Processing**
   1. Taking into account the state of the art and the high sensitivity of the Personal Data, Vendor 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). In particular, the Vendor shall take the Minimum Security Measures as listed under **Exhibit B** to this Addendum.
   2. In assessing the appropriate level of security, Vendor shall take account, in particular, of the risks that are presented by the nature of such Processing activities, and particularly those related to possible Personal Data Breaches.
   3. Without limiting clauses 5.1 and 5.2, Vendor shall, and shall cause each Processor or Sub-Processor to, comply with the security obligations set out in the Addendum including **Exhibit B**.
3. **Sub-processing**

***When Vendor is acting as a Processor or Sub-Processor*:**

* 1. Billtrust authorizes Vendor to appoint (and permit each Sub-Processor appointed in accordance with this Section [6](#_heading=h.4d34og8) to appoint) Sub-Processors in accordance with this Section [6](#_heading=h.4d34og8) and any possible further restrictions, as set out in the Agreement, as the case may be.
  2. Vendor may continue to use those Sub-Processors already engaged by Vendor as of the date of this Addendum, subject to Vendor meeting the obligations set out in Section 6.5. The list of Vendor’s Sub-Processors as of the Effective Date is provided in **Exhibit C** to this Addendum.
  3. Subject to Section 6.2, Vendor shall notify Billtrust in advance of appointing any new Sub-Processors no less than 90 days of their proposed first use for Processing under the Agreement. Within 30 days after Vendor’s notification of the intended change, Billtrust can object to the addition of a Sub-Processor on the basis that such addition would violate (i) Applicable Data Protection Laws; (ii) cause Billtrust to violate its contractual obligations with a third party; or (iii) other reasonable cause. Billtrust’s objection must be in writing and include any specific reasons for its objection and options to mitigate. If Billtrust does not object within such period, the Sub-Processor may be engaged by Vendor without further notice.
  4. If Billtrust reasonably objects to a proposed appointment as set out in Section 6.3, 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. If no solution can be found which is satisfactory to both parties, Billtrust, upon written notice to Vendor, may terminate the 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.
  5. With respect to each Sub-Processor, Vendor shall:
     + 1. before the Sub-Processor first Processes Personal Data (or, where relevant, in accordance with Section [6.2](#_heading=h.17dp8vu)), 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 Data Protection 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 Vendor 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 Data Protection Laws.
  6. Where any Sub-Processor fails to fulfil its data protection obligations under such written contract (or in the absence thereof, as the case may be), Vendor shall remain fully liable to Billtrust for the performance of the respective Sub-Processors’ obligations under such contract or in connection with this Addendum.

1. **Rights of the Data Subjects**
   1. When acting as Processor or Sub-Processor, taking into account the nature of the Processing, Vendor shall assist Billtrust (and for Customer Personal Data: the Customer) 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 Data Protection Laws.
   2. With regard to the rights of the Data Subjects within the scope of this Section 7, Vendor 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 Data Protection Laws to which the Personal Data Recipient is subject, in which case Vendor shall, to the extent permitted by Applicable Data Protection 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 Data Protection Laws.
2. **Personal Data Breach**

***When Vendor is acting as a Processor or Sub-Processor*:**

* 1. If Vendor discovers, is notified of, or has reason to suspect a Personal Data Breach affecting Personal Data, Vendor will provide notice to Billtrust within 24 hours of becoming aware of a confirmed or suspected Personal Data Breach.
  2. Vendor 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 Data Protection Laws, including any obligations to report the Personal Data Breach to the competent supervisory authorities, and/or inform the Data Subjects.
  3. Vendor shall co-operate with Billtrust and take all reasonable commercial steps (at Vendor’s own expense) to assist Billtrust in the investigation, mitigation, and remediation of each such Personal Data Breach.

1. **Data Protection Impact Assessment and Prior Consultation**
   1. For services that the Vendor provides as Processor or Sub-Processor, Vendor 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 Data Protection 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.
2. **Deletion or Return of Personal Data**
   1. Vendor 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 Data Protection Laws require storage of any such Personal Data.
   2. Vendor 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 Data Protection Laws require storage of any such Personal Data. In the event that Billtrust has not specified its choice, it shall be deemed that Vendor is obliged to delete all Personal Data from Billtrust.
   3. Vendor 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.
   4. Upon request from Billtrust, Vendor shall provide written certification to Billtrust that it has fully complied with this Section 10.
3. **Audit Rights**
   1. Billtrust may request, and Vendor will provide (subject to obligations of confidentiality), all information reasonably necessary to demonstrate compliance with the obligations set forth in this Addendum and Applicable Data Protection Laws, including but not limited to a current SOC 1/2 audit report, ISO 27001 certificate, or other substantially similar third party certification or audit of industry standard.
   2. If Billtrust after having reviewed such audit report(s), still deems that it requires additional information (for example, Vendor’s policies and procedures regarding data protection, information from Vendor’s Sub-Processors, or any other relevant information) Vendor 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 Data Protection Laws.

***When acting as a Processor or Sub-Processor***:

* 1. In addition, Vendor shall reasonably 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.
  2. Billtrust shall give reasonable notice of any audit or inspection to be conducted under section 11.3 and agree to subject such audit or inspection to the Vendor’s security policy and other confidentiality requirements, where legally permissible.
  3. If it is established during an audit that Vendor has failed to comply with its obligations under this Addendum, Billtrust shall notify Vendor and Vendor shall take all measures necessary to ensure its compliance as soon as reasonably practicable.
  4. Billtrust shall bear its own third party costs in connection with such inspection or audit, unless the findings of the audit show that Vendor and/or any Sub-Processor failed to comply in any material respect with the provisions of this Addendum, in which case Vendor shall reimburse all reasonable and documented costs incurred by Billtrust in connection with such inspection or audit.

1. **Jurisdiction Specific Terms**
   1. To the extent Vendor processes Personal Data originating from, or protected by, Applicable Data Protection Laws in one of the jurisdictions listed in **Exhibit D**, then the terms specified in **Exhibit D** 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 D** from time to time, to reflect changes in or additions to Applicable Data Protection Laws to which Billtrust is subject. If Billtrust updates **Exhibit D**, it will provide the updated **Exhibit D** to Vendor. If Vendor does not object to the updated **Exhibit D** within 30 days of receipt, Vendor will be deemed to have consented to the updated **Exhibit D**.
   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. When acting as Processor or Sub-Processor, Vendor acknowledges and confirms that it does not receive any Personal Data as consideration for any services or other items that Vendor provides to Billtrust. Billtrust retains all rights and interests in Personal Data. Vendor agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Vendor to qualify as selling or sharing Personal Data under Applicable Data Protection Laws.
3. **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 Vendor 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 Data Protection 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 prevail. This is without prejudice to the order of precedence between the Jurisdiction Specific Terms and any other provision in this Addendum including Section 12.3 above.
   4. Should any provision of this Addendum or its 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.
   5. If Vendor 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 Vendor materially breaches this Addendum, or suffers a material Personal Data Breach, Billtrust may, upon written notice to the Vendor, 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.
   8. This Addendum and its exhibits is governed by the laws that apply to the Agreement. Any disputes between the Vendor 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.

# Exhibit A: Details of processing

1. **List of Parties**

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

Contact details: [privacy@billtrust.com](mailto:privacy@billtrust.com), see signature section of this Addendum for additional details.

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

Role:

- For **Billtrust Personal Data**, Controller: see Processing Annex 1

- For **Customer Personal Data**, Processor: see Processing Annex 2:

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

Contact details: See signature section of this Addendum for additional details.

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

Role:

- For **Billtrust Personal Data**, Parties have agreed that Vendor’s role for the Services set out in the Agreement is: Processor

- For **Customer Personal Data**: a Sub-Processor (the Parties acknowledge and agree that Billtrust supplies a service to its Customers, and that Billtrust has appointed Vendor in connection with such services pursuant to the Agreement).

1. **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 two categories of data envisaged by this Agreement:

Processing Annex 1: Billtrust Personal Data, Controller to Processor

Processing Annex 2: Customer Personal Data, Processor to Sub-Processor

**Processing Annex 1 –**  **Billtrust Personal Data**

This Processing Annex describes PersonalData transferred by Billtrust as Controller and Data Exporter(s) and the purposes for which that Personal Data may be Processed by the Vendor as Data Importer(s) in the role of Processor.

| Categories of data subjects whose personal data is transferred: | Categories of data subjects are defined in the Agreement. For the avoidance of doubt, categories include:  Billtrust Employees - Past, present and future staff of the Data Exporter (including volunteers, agents, independent contractors, interns, temporary and casual workers).  For Agreements related to our human resources recruitment, also included is the category of Job candidates and applicants of the Data Exporter.  For Agreements related to our marketing and events also included is staff of past, present and potential users of Billtrust Services (including those that attend or sign up for Billtrust events or conferences).  Other (option to add) |
| --- | --- |
| Categories of personal data transferred: | Categories of personal data transferred are defined in the Agreement. For the avoidance of doubt, categories include:  *Billtrust Employees*  Identification data: e.g. civil/marital status, photograph, nationality, corporate and national identifier, IP address; personal and business contact details: e.g. address, telephone number, email address, fax number, emergency contact information.  *For Agreements related to our human resources*, also included is personal details and identification data; employment details: e.g job title, company name, grade, occupation code, geographic location; national identifiers; e.g. national ID/passport number, visa or immigration status; academic and professional qualifications; financial data.  *For Agreements related to our marketing and events, also included is p*ersonal detail and business contact information: name; e-mail address; phone number; office address; Name of employer; job title; IT-related data: IP addresses of visitors to the Data Exporter's websites; correspondence data and other communications.  Other (option to add) |
| Sensitive data transferred (if applicable) and applied restrictions or safeguards, or additional security measures: | Billtrust does not anticipate the collection of any sensitive data as a Controller from any individuals other than Billtrust employees in connection with valid employment purposes. Such collection will only concern limited sensitive data, for example, health-related information for the purpose of managing employee absences, or disabilities in order to provide access to our premises.  Race and ethnicity may appear indirectly on photos and other information available on passports and national IDs, which are necessary to comply with local immigration laws and for employee travel management. However, race/ethnicity are not Processed purposefully in Europe.  Trade union membership may be collected but only where permitted and for the purposes defined under Applicable Data Protection Laws.  The Parties will only export sensitive data where such export is not otherwise restricted by Applicable Data Protection Laws.  The safeguards are set out in Exhibit B. |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): | Continuous |
| Nature of the processing: | Vendor will process the Personal Data to deliver the Services pursuant to the Agreement. |
| Purpose(s) of the data transfer and further processing: | The Data Importer will provide assistance to Data Exporter in undertaking that Processing. |
| 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 section 10.Deletion or Return of Personal Data. |
| 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. |

**Processing Annex 2 - Billtrust Customer Personal Data**

This Annex describes the types of Customer PersonalData transferred to a Vendor when Billtrust and/or Billtrust Affiliates act as a Processor and Vendor acts as Sub-Processor. This Annex also describes the purposes for which such CustomerData may be Processed..

| Categories of data subjects whose personal data is transferred: | Data subjects of which a Billtrust Customer is the Controller, which includes users of the Billtrust products and services e.g. Customer’s employees, employees of the customer of the Billtrust Customer, and other Customers’ users of the services (whether current, past or potential). |
| --- | --- |
| Categories of personal data transferred: | The categories of Personal Data to be Processed are personal identifiers and business contact information, including business address and email address, first and last name, login credentials; financial information such as credit card company, credit card number and expiration date, credit card billing address, bank account information; invoicing information and order data; IT information such as user log-in and information from the products and services. |
| Sensitive data transferred (if applicable) and applied restrictions or safeguards, or additional security measures: | Billtrust does not anticipate the processing of any sensitive data with respect to Customer data.  The safeguards are set out in Exhibit B. |
| The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): | Continuous. |
| Nature of the processing: | Vendor will process the Personal Data to deliver the Services pursuant to the Agreement. |
| Purpose(s) of the data transfer and further processing: | The purpose of processing of Customer Personal Data pertains to the provision of specified products and services implementation under the Agreement. |
| The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: | For as long as (i) the Data Exporter (Billtrust) and Data Importer (Vendor) have an Agreement for Services and (ii) the Data Exporter (Billtrust) provides services to its Customer which require the Processing of Billtrust Customer Data. |
| 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 and this Addendum. 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. |

1. **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: Minimum Security Measures

**Vendor Information Security Requirements**

**A. INTRODUCTION**

These Vendor Information Security Requirements (“Requirements”) describe Vendor’s obligations with respect to information security and data protection in relation to the Services provided by Vendor to Billtrust under the Agreement between Billtrust or Billtrust’s affiliate(s) and Vendor. For the purpose of these Requirements, the term “Vendor” shall mean a third-party providing Software or Services to Billtrust or a Billtrust Customer and who is identified by either their entity name or the defined terms “Vendor”, “Service Provider”, “Supplier”, “Provider”, or “Consultant” in the Agreement. Terms capitalized and used in these Requirements will have the meanings ascribed to them under the Addendum unless specifically provided for in these Requirements otherwise. In the event an entity other than Vendor does so under a contract with Vendor or otherwise for or on behalf of Vendor, Vendor will ensure by contract or otherwise that the following provisions apply correspondingly to the other entity for the benefit of Billtrust.

For the avoidance of doubt, to the extent of any conflict or inconsistency between the provisions of this Addendum and any of the Requirements listed below, the Requirements shall prevail and take precedence over such conflicting or inconsistent provisions in this Addendum, subject to Exhibit D, clause 1.3(e).

**B. SECURITY MEASURES**

1. Billtrust acknowledges and agrees that Vendor may change its security policies and related security measures, provided that Vendor maintains, at all times, an overall level of security as least as stringent as the one set forth in this Addendum.

2. The Vendor Processes Personal Data in accordance with applicable law to which Processor is subject and in accordance with the data security requirements of the controls defined by latest available SSAE 18 SOC 2 or ISO 27001 implemented controls (or equivalent standard).

3. Comprehensive security policies, standards and procedures are developed and maintained by a designated person responsible for privacy and data protection, such as a Chief Security Officer, and reviews of the information security policy are completed at least annually.

4. The Vendor must provide its personnel, third party consultants, and contractors with annual information security awareness training including, but not limited to, education on general safety awareness, relevant security policies and procedures, and Personal Data Processing.

**C. ACCESS CONTROL**

1. Vendor shall maintain suitable measures in order to prevent unauthorized persons from gaining access to the data Processing equipment (namely database and application servers and related hardware) where the Personal Data is Processed or used. This is accomplished by measures like:

* establishing security areas and establishing procedures for working in such areas;
* protection and restriction of access paths;
* securing the data Processing equipment and personal computers;
* establishing access authorizations and appropriate restrictions to authorized personnel;
* all access to the data centre where Personal Data is hosted is logged, monitored, and tracked;
* the data centre where Personal Data is hosted is secured by a security alarm system; and
* other appropriate security measures.

2. The Vendor manages information system accounts by implementing centralized control of user access and administrator functions; access is assigned and periodically reviewed to ensure least privilege access is granted.

3. Where the Vendor (a) stores, processes, or transmits Payment Card Data in connection with the Services under the Agreement, or (b) is otherwise subject to PCI DSS, computing systems processing credit card (PAN) and ACH information must be physically and/or logically isolated to reduce the risk of unauthorized access.

4. The Vendor maintains suitable measure to prevent its systems from being used by unauthorized persons, such as:

* annual review and certification of logical access accounts;
* log file of events (monitoring of break-in-attempts);
* issuing and safeguarding of identification codes;
* employee policies and training with respect to each employee's access rights to Personal Data (if any), including informing employees about their obligations and the consequences of any violations of such obligations, to ensure that employees will only access Personal Data and resources required to perform their job duties;
* all access to data content is logged and monitored;
* users with access to Vendor's information resources must utilize User IDs that are specifically assigned to them;
* controls minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts;
* -processes and procedures for password strength requirements are in line with applicable regulatory or industry guidelines;
* -effective and measured disciplinary action against individuals who access Personal Data without authorization;
* release of Personal Data only to authorized persons;
* control of files, controlled and documented destruction of Personal Data; and
* policies controlling the retention of back-up copies.

**D. AVAILABILITY CONTROL**

1. Vendor shall maintain suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This is accomplished by:

* infrastructure redundancy;
* tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for database server;
* complying with Processor’s business continuity policy; and
* any detected security incident is recorded.

**E. INPUT CONTROL**

Vendor implements suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been input into Personal Data Processing systems or removed. This is accomplished by:

* an authorization policy for the input of data into memory, as well as for the reading, alteration and disposal of stored Personal Data;
* authentication of the authorized personnel;
* protective measures for the data input into memory, as well as for the reading, alteration and disposal of stored Personal Data;
* utilization of user codes (passwords);
* following a policy according to which all employees of Vendor who have access to Personal Data Processed for Billtrust shall reset their passwords at a minimum once in a 180 day period, or as defined in Processor’s IT Security Policy and in line with potential multi-factors of authentication;
* providing that entries to Processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
* automatic log-off of user IDs that have not been used for a substantial period of time;
* proof established Vendor’s organization of the input authorization; and
* electronic recording of entries.

**F. OPERATIONS MANAGEMENT**

1. Vendor information resources are established and maintained in accordance with information technology standard builds and the applicable platform-specific security baseline.

2. Vendor is responsible for installing available patches on the information resources under their control in a timely fashion after the release. Critical security patches relevant to the protection of sensitive information (including Personal Data) must be installed as soon as reasonably possible after release.

3. Vendor will perform vulnerability scans and penetration tests on a periodic basis and no less than annually.

4. Vulnerability remediation efforts, including patch implementations, must be coordinated and processed according to the Vendor’s change management process, including meeting all testing and/or documentation requirements.

5. System lifecycle and change management processes and controls are established.

6. Development, test and production environments must be separated physically, or at a minimum logically, to reduce the risk of accidental change or unauthorized access to production software and data.

7. The Vendor must establish processes and procedures for separation of duties between development/test and production environments.

8. Vendor maintains a change control process for the change of backup and restore documentation and deploys appropriate technologies to manage backup and restore tasks.

9. The Vendor must establish processes and procedures for virus detection software configuration.

10. Information resources are backed up and can be recovered in a timely manner.

11. The Vendor must establish a record retention schedule that supports regulatory requirements.

12. The Vendor employees, third party contractors and vendors must adhere to all copyright laws and packaged software license agreements.

13. Configuration management and software standards are established.

**G. SECURITY DEFENSE, MONITORING, AND RESPONSE**

1. The Vendor is responsible for developing, implementing, maintaining and communicating a security incident reporting process and related procedures to include, without limitation, all security and privacy related incidents involving a 'breach of security' to Personal Data.

**H. SECURING DATA IN TRANSIT AND AT REST**

1. Encryption use standards are established to protect sensitive information (including Personal Data) when being transmitted and/or stored on Vendor information resources. Where applicable, Primary Account Number (PAN) must be encrypted both at rest and in transit.

2. Connections to wireless access points must be authenticated over an industry best practice, strong encrypted channel.

3. Sensitive information, including Personal Data, such as cardholder information, must not be sent over the Internet, via Remote Access or transmitted over public or external networks unless the transition utilizes a strong encryption method or protocol as designated by NIST.

**I. SERVER AND NETWORK SECURITY**

***This section is only applicable if Vendor is (a) storing or processing Billtrust Customer data, on its network, or (b) remotely accessing Billtrust Customer data or network access credentials in connection with the Services under the Agreement.***

1. Vendor will harden its operating systems in accordance with leading information security industry standards (e.g., NIST) and adhere to the concept of “least-privileged” access.

2. Requirements are established for ensuring users only have direct access to the network services for which they have been specifically authorized to use and only authorized devices are permitted to connect to the network.

3. Vendor will have mechanisms to prevent the unauthorized removal of Billtrust Customer Data from the Vendor’s networks.

4. Vendor will employ a defensive model when building networks (including firewalls) in a multi-tiered approach and use separate layers of presentation, business logic and data when considered necessary in accordance with information security best practices. Connection between networks shall be limited to those ports and services required for Vendor to support, secure, monitor and perform the Services under the Agreement.

5. Where the Services are provided using online services, the Vendor must establish and implement a firewall rule base to prohibit traffic which is not specifically permitted for valid business purposes and ensure that adequate protection is in place.

**J. THIRD PARTY SERVICES**

1. The Vendor must establish processes and procedures for analysis of services to be outsourced.

2. The Vendor must evaluate and perform thorough due diligence before engaging a Vendor.

3. Depending on the sensitivity and criticality of the services provided, the Vendor requests or commissions a review of the service provider's security control structure.

4. The Vendor employs safeguards to ensure that the interests of Vendors are consistent with and reflect Vendor interests.

5. A written agreement containing the appropriate terms and conditions must be executed for all third party service provider relationships.

**K. APPLICATION MANAGEMENT**

***For all applications supported by the Vendor in connection with the Services under the Agreement., the following controls will be implemented:***

1. The Vendor requires the integration of security requirements in system design that are consistent and supportive of the Vendor security architecture.

2. Suitable measures are in place to prevent the disclosure of (i) application configuration information that could be exploited; and (ii) Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof.

3. The Vendor implements processes and procedures for testing of security features and controls as part of application testing.

4. Significant modifications, major enhancements, and new systems must be integration tested prior to deployment in production environments.

**L. ENTERPRISE RESILIENCE (BUSINESS CONTINUITY)**

***This section is only applicable if Vendor is (a) storing or processing Billtrust Customer Data on its network, or (b) providing Billtrust with a Service or Software that Billtrust relies upon to deliver services to its Customers.***

1. Vendor will establish and maintain disaster recovery and business continuity plans, including offsite data storage and recovery infrastructure, designed to minimize the risks associated with a disaster affecting Vendor’s ability to provide the Services.

2. Vendor will maintain adequate backup procedures in order to recover data it processes in connection with the Services; test its disaster recovery and business continuity plans, not less frequently than annually, and will provide to Billtrust its annual disaster recovery and business continuity plans test results upon request.

**M. COMPLIANCE**

1. The Vendor must establish processes and procedures for documentation of legal and compliance obligations including privacy and data protection.

3. Personal Data must only be obtained by Vendor for specified and lawful purposes and must not be further processed or disclosed if prohibited by law.

4. The Vendor must have procedures for the data subjects to exercise their rights relating to their Personal Information held by Vendor, although with respect to this Agreement, Billtrust or the Billtrust Customer has primary responsibility for responding to data subjects.

5. When outsourcing to a third party, the protection of Personal Data is considered.

6. The Vendor conducts independent and/or self-administered audits, assessments and penetration tests on an annual basis, or as otherwise necessary (i.e. segmentation controls, significant infrastructure or application upgrade or modification).

# Exhibit C: List of Sub-Processors

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

| **Sub-Processor**  **(full legal entity name)** | **Processing Activities** | **Categories of Billtrust Personal Data** | **Location**  **(country)** |
| --- | --- | --- | --- |
| |  | | --- | | Auth0 | | AWS | | FiveTran | | FIS/Global/Vantiv | | Looker | | Slack | | Snowflake | | Zendesk |   Option to add | |  | | --- | | Spreedly direct customer portal login | | Cloud data processing | | SaaS data integration service | | Account updater service | | Business intelligence and visualization for analytics | | Private customer communication | | Data warehousing | | Inbound customer support and help center/community | |  | |  | | --- | | USA | | USA | | USA | | UK | | USA | | USA | | USA | | USA | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Exhibit D: Jurisdiction-Specific Terms

1. **Transfers of EEA Personal Data**
   1. Definitions:

For the purpose of interpreting the current Section 1 (Transfers of EEA Personal Data) of **Exhibit D**, the following terms shall have the meanings set out below:

* 1. “**EEA**” means the European Economic Area..
  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. “**Supervisory Authority**” in the context of the GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.
  4. “**Third Country**” (as used in this Section) means a country or territory outside of the EEA.
  5. Transfer Mechanisms:

With regard to any EEA Restricted Transfer from Billtrust to Vendor 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 Personal Data is to be transferred ensures an adequate level of data protection;
  2. 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.
  5. Standard Contractual Clauses:
     + 1. To the extent that Billtrust acts as Controller and Vendor acts as Controller, Vendor (which will take on the obligations of “data importer” for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:
          1. Module One of the Standard Contractual Clauses will apply;
          2. in Clause 7, the optional docking Clause will not apply;
          3. Clause 9, shall be deemed inapplicable;
          4. Clause 13, all square brackets removed, and all text therein is retained;
          5. Clause 17, the parties agree that the SCCs will be governed by the laws indicated under Section 14.8 of the Addendum;
          6. in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;
          7. 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.
          8. the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.
       2. To the extent that Billtrust acts as Controller and Vendor acts as Processor, Vendor (which will take on the obligations of “data importer” for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:
          1. **Module Two** of the Standard Contractual Clauses will apply;
          2. in Clause 7, the optional docking Clause will not apply;
          3. in Clause 9, Option 1 Specific Prior Authorisation applies;
          4. in Clause 11, the optional language will not apply;
          5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws indicated under Section 14.8 of the Addendum;
          6. in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;
          7. 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.
          8. the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.
          9. in Annex I:

Part A: with the information set out in the Exhibit A to this Addendum;

Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and

Part C: in accordance with the criteria set out in Clause 13(a) of the EU SCC’s;

* + - * 1. Annex II: with the Minimum Security Measures of Exhibit B.
      1. To the extent that Billtrust acts as Processor and Vendor acts as Sub-Processor, Vendor (which will take on the obligations of “data importer” for the purposes of the Standard Contractual Clauses) and Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) hereby enter into the Standard Contractual Clauses, which are incorporated by this reference and constitute part of this Addendum (and where Annexes 1 and 2 of the Standard Contractual Clauses would reflect the information as contained **Exhibit A** to this Addendum) as follows:
         1. **Module Three** will apply;
         2. in Clause 7, the optional docking Clause will not apply;
         3. in Clause 9, Option 1 Specific Authorisation applies;
         4. in Clause 11, the optional language will not apply;
         5. in Clause 13, all square brackets removed, and all text therein is retained;
         6. in Clause 17, Option 1 will apply, and the SCC’s will be governed by the laws indicated under Section 14.8 of the Addendum;
         7. in Clause 18(b), disputes shall be resolved before the competent courts pursuant to Section 14.8 of the Addendum;
         8. 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.
         9. the audits described in clause 8.9 of the SCCs shall be carried out in accordance with Section 11 of this Addendum.
         10. in Annex I:

Part A: with the information set out in Exhibit A to this Addendum;

Part B: with the relevant Processing Annex(ures) set out in Exhibit A to this Addendum; and

Part C: in accordance with the criteria set out in Clause 13(a) of the EU Standard Contractual Clauses;

* + - * 1. Annex II: with the Minimum Security Measures of Exhibit B
      1. 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 E** to this Addendum serves to supplement the Standard Contractual Clauses.
  1. In cases where the Standard Contractual Clauses apply, and there is a conflict between the terms of the Addendum, the Supplemental Clauses to the Standard Contractual Clauses contained in Exhibit E and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

1. **California**
   1. Definitions:

For the purpose of interpreting the current Section 2 (California) of Exhibit D, the following terms shall have the meanings set out below:

* 1. “**Applicable Data Protection Laws**” includes the CA Privacy Laws (as defined below) as may be amended from time to time.
  2. “**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.
  3. 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 current Section 2 (California) of Exhibit D, the following terms shall be interpreted as follows:

* + - 1. “**Contractor**” has the meaning given to it in Section 1798.140(j) of the California Civil Code.
      2. “**Personal Data Breach**” includes “Breach of the Security of the System” as defined in Section 1798.8 of the California Civil Code;
      3. “**Personal Data**” includes “Personal Information” as defined in Section 1798.140(o) of the California Civil Code.
      4. “**Service Provider**” in Section 1798.140(ag) of the California Civil Code.

Where Vendor acts as a Service Provider or Contractor on behalf of Billtrust in accordance with Section 3 of the Addendum:

* 1. Billtrust discloses Personal Data to Vendor solely for: (i) valid Business Purposes; and (ii) to enable Vendor to perform the Processor Services under the Agreement(s).
  2. Vendor shall not:
     1. sell or share Personal Data it collects from Billtrust pursuant to the Agreement(s);
     2. retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) for any purpose other than providing the Processor Services specified in the Agreement(s) or as otherwise permitted by the CA Privacy Laws;
     3. retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) for any commercial purpose other than the business purpose(s) specified in the Agreements (or in any applicable statement of work or similar document), unless expressly permitted by the CA Privacy Laws;
     4. retain, use or disclose Personal Data it collects from Billtrust pursuant to the Agreement(s) outside the direct business relationship between it and Billtrust unless expressly permitted by the CA Privacy Laws. For example, Vendor may not combine or update Personal Data collected pursuant to the Agreement(s) with personal information that it received from another source or collected from its own interaction with a consumer, unless expressly permitted by the CA Privacy Laws.
  3. Vendor shall comply with all applicable sections of the CA Privacy Laws, including with respect to the Personal Data collected pursuant to the Agreement(s), providing the same level of privacy protection as required of Billtrust by the CA Privacy Laws.
  4. Vendor grants Billtrust the right to take reasonable and appropriate steps to ensure that it uses the Personal Data collected pursuant to the Agreement(s) in a manner consistent with Billtrust’s obligations under the CA Privacy Laws.
  5. Vendor shall notify Billtrust after it makes a determination that it can no longer meet its obligations under the CA Privacy Laws.
  6. Vendor grants Billtrust the right, upon notice, to take reasonable and appropriate steps to stop and remediate its unauthorized use of Personal Data.
  7. Vendor shall enable Billtrust to comply with consumer requests made pursuant to CA Privacy Laws or Billtrust shall inform Vendor of any consumer request made pursuant to the CA Privacy Laws that it must comply with and provide the information necessary for Vendor to comply with the request.
  8. To the extent Vendor subcontracts with another person in providing services to Billtrust, Vendor shall have a contract with the subcontractor that complies with the CA Privacy Laws.
  9. Vendor certifies that it understands these restrictions and will comply with them.

1. **Canada**
   1. Definitions:

For the purpose of interpreting the current Section 3 (Canada) of Exhibit D, 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.
  6. **Necessary Consent.** When acting as Controller, Billtrust confirms that is has obtained a valid consent (as defined under PIPEDA), where necessary to Process Personal Data of each Data Subject.

1. **Switzerland**
   1. Definitions:

For the purpose of interpreting the current Section 4 (Switzerland) of Exhibit D, 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.
  9. **Swiss Restricted Transfers.** With regard to any Swiss Restricted Transfer from Billtrust to Vendor within the scope of this Addendum, one of the following transfer mechanisms shall apply, in the following order of precedence:
  10. 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;
  11. Vendor’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;
  12. the Standard Contractual Clauses (insofar as their use constitutes an “appropriate safeguard” under the FADP and the OFADP, as the case may be); or
  13. any other lawful basis, as laid down in FADP and the OFADP, as the case may be.
  14. Standard Contractual Clauses:
  15. Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) and Vendor (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 E** to this Addendum serves to supplement the Standard Contractual Clauses.
  16. 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.
  17. Where the Standard Contractual Clauses apply, Billtrust 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.
  18. The FDPIC shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the FADP.
  19. 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.
  20. The SCCs also protect the data of legal entities until the entry into force of the revised version of the FADP of 25 September 2020, which is scheduled to come into force in 2023.

1. **United Kingdom** 
   1. Definitions:

For the purpose of interpreting the current Section 4 (United Kingdom) of Exhibit D, 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”** means the United Kingdom of Great Britain and Northern Ireland;
  3. **“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).
  4. **“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”).
  5. “**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.
  6. UK Restricted Transfers:

With regard to any UK Restricted Transfer from Billtrust to Vendor 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. Vendor’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) as varied by the UK Transfer Addendum in the manner described below in section 5.3 (d); or
  4. any other lawful basis, as laid down in the UK GDPR and the Data Protection Act 2018, as the case may be.
  5. Standard Contractual Clauses:
  6. Billtrust (which will take on the obligations of “data exporter” for the purposes of the Standard Contractual Clauses) and Vendor (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.
  7. 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 E** to this Addendum serves to supplement the Standard Contractual Clauses.
  8. 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.
  9. PART 1 OF THE UK TRANSFER ADDENDUM. As permitted by Section 17 of the UK Transfer Addendum, the parties agree that:
     1. (i) Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed completed with the corresponding details set out in **Exhibit A** to this Addendum and the foregoing provisions of Exhibit D, section 1.3 (subject to the variations effected by the Mandatory Clauses described in (b) below); and

(ii) Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled ‘Data Exporter’ being deemed to have been ticked.

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

# EXHIBIT E: Supplemental Clauses to the Standard Contractual Clauses

By this **Exhibit E** (this “Exhibit”), the Parties provide additional safeguards to and additional redress to the Data Subjects to whom transferred Personal Data pursuant to Standard Contractual Clauses. 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:
   2. “**Data Importer**” and “**Data Exporter**” shall have the same meaning assigned to them in the Standard Contractual Clauses concluded by the Parties.
   3. “**FISA**” means the U.S. Foreign Intelligence Surveillance Act.
   4. “**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. **Back doors**
   1. Data Importer certifies that:
   2. it has not purposefully created back doors or similar programming that could be used to access Data Importer’s Systems or Personal Data subject to the Standard Contractual Clauses;
   3. it has not purposefully created or changed its business processes in a manner that facilitates access to Personal Data or systems, and
   4. 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.
   5. 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.
   6. In circumstances where the Data Importer disclosed Personal Data transferred in violation of the commitments contained in provision 3.1 above, Data Importer shall compensate Data Subjects for any material and non-material damage suffered as a result of such violation.
4. **Other Measures to Prevent Authorities from Accessing Personal Data**
   1. Notwithstanding the application of the Minimum Security Measures set forth in the Addendum **Exhibit B**, Data Importer will implement:
   2. Internal policies or procedures establishing that:
      * + 1. 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;
          2. 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;
          3. if Data Importer is legally required to comply with an order, it will respond as narrowly as possible to the specific request; and
          4. Data Importer shall monitor any legal or policy developments (such as changes in the legislation or practice in the countries where the data is transferred) which might lead to its inability to comply with its obligations under the SCCs. In particular, Data Importer shall make reasonable efforts to inform Billtrust of legal or policy developments ahead of their implementation to enable Billtrust to recover the Personal Data from the Data Importer (either by returning the data to Billtrust or by deleting or securely encrypting the data).
5. **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** | |  | Spreedly, Inc. **(Vendor)** | |
| --- | --- | --- | --- | --- |
|  | |  |  | |
| **Signature** | |  | **Signature** | |
|  | |  |  | |
| **Name** | |  | **Name** | |
|  | |  |  | |
| **Title** | |  | **Title** | |
|  | |  |  | |
| **Date** | |  | **Date** | |
|  |  | | |
|  |  | | |

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