GDPR Data Processing Addendum

between

1. ______________________________________, (the **"Controller"**); and
Email address (Sync username)

2. Sync.com Inc. (the **"Processor"**)

(together the "Parties").

---

1 - Scope of Application

In the course of rendering services as per the Processor's (Sync.com Inc.) Terms of Use, the Processor processes personal data and encrypted data provided by the Controller, with regard to which the Controller acts as controller in terms of applicable data protection law ("Controller Data"). This Addendum specifies the data protection obligations and rights of the parties in connection with the processing of Controller Data to render the services under the Terms of Use.

2 - Scope of the commissioning / Right of the Controller to issue instructions

2.1 - The Processor shall process Controller Data on behalf of and in accordance with the instructions of the Controller, unless the Processor is legally required to do so. In the latter case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.2 - The processing of Controller Data by the Processor comprises exclusively of personal data and other contact information provided during account creation, and personal and encrypted data provided during use of the service. The duration of processing corresponds to the duration of the Terms of Use.

The Processor's account creation process requires that the Controller provide personal information and other contact information. Such personal information may include e-mail address, first name, last name, and personal and/or business billing information. Personal information will be processed by the Processor for verification purposes and to provide services to the Controller.

Personal information and other information provided by the Controller is encrypted in transit using SSL/TLS encryption. The Processor may apply an additional layer of client side encryption automatically, during transit and at rest, which is defined as end-to-end encryption. The Processor never processes file, file meta data, encryption keys or passwords ("Encrypted Controller Data") in an unencrypted format, unless the Controller requests the Processor to do so. Encrypted Controller Data is always end-to-end encrypted, and stored in such a way that the Processor cannot access it in a readable format, or share it with third-parties. Sync's applications and features allow the Controller, and only the Controller (or in the case of the Business Pro plan, the Controller and the Controller's administrator) to control who can decrypt and access Encrypted Controller Data, for example when sharing, when enabling in-app sharing with other apps, when enabling account or password recovery, or in the case of a Business Pro plan administrator, when provisioning an account.

The Processor makes every effort to ensure that the Processor cannot access or decrypt the Controller's Encrypted Controller Data, regardless of which features the Controller may have enabled or use.

During the use of the service, the Controller may also submit non-Encrypted Data, including email addresses when sharing. The Processor makes every attempt to ensure that the transmission and storage of non-Encrypted Data is secure, and that access to this data is highly restricted. If the Controller has any questions about the security of Encrypted Controller Data or non-Encrypted Data the Controller can contact the Processor at help@sync.com

2.3 - The Controller reserves the right to issue instructions about the type, extent, purpose and means of the processing of Controller Data. If and insofar as the Terms of Use contain provisions on change requests, such provisions shall apply to these instructions mutatis mutandis.

2.4 - The Controller shall be responsible for the lawfulness of the processing of the Controller Data. In case third parties assert a claim against the Processor based on the unlawfulness of processing Controller Data, the Controller shall release the Processor of any and all such claims upon the Processor's first request.

2.5 - The Processor reserves the right to anonymize the Controller Data or to aggregate data in a way which do not permit the identification of the user or natural persons, as well as the right to use the data in this form for purposes of designing, further developing, optimizing and providing the service to the Controller as well as to other users of the service. The parties agree that the Controller Data rendered anonymous or aggregated as above-mentioned are no longer classified as Controller Data in terms of this Addendum.

3 - Obligation of the Data Controller

The Data Controller agrees and warrants:

That the Personal Data processed by the Data Controller and transferred to the Data Processor is carried out in accordance with the Applicable Law, including the legislative requirements regarding lawfulness of processing.

That for the duration of the personal data-processing services, it has instructed and will instruct the Data Processor to process the personal data transferred only on the Data Controller's behalf and in accordance with Applicable Law.

That it ensures sufficient guarantees in respect of Data Controller's internal technical and organizational security measures and safeguards of Personal Data.

That it ensures implementation and enforcement of policies and procedures regarding sharing and collaboration of Personal Data using the Data Processor's services.

4 - Personnel requirements

4.1 - The Processor shall obligate all personnel engaged in the processing of Controller Data to confidentiality with regard to processing of Controller Data.

4.2 - The Processor shall ensure that natural persons acting under his authority who have access to Controller Data shall process such data only on his instructions.

5 - Security of processing

5.1 - The Processor takes all appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the nature, the scope, circumstances and purposes of the processing of Controller Data, as well as the different likelihood and severity of the risk to the rights and freedoms of the data subject, in order to ensure a level of protection appropriate to the risk of Controller Data.

5.2 - In particular, the Processor shall establish prior to the beginning of the processing of Controller Data and maintain throughout the term technical and organizational safeguards to protect the Data Controller's Personal Data in delivering the Services as described in the Terms of Use, and ensure that the processing of Controller Data is carried out in accordance with those measures.

Encryption

the Data Processor makes every attempt to encrypt Personal Data during transit and at rest.

Account Security

The Data Processor provides the Data Controller with optional account security features including two-factor authentication, to guard against unauthorized account level changes.

Data Security

The Data Processor provides the Data Controller with security, compatibility and account recovery features to control who can decrypt and access Encrypted Controller Data.

Data Recovery

The Data Processor provides the Data Controller and its end users the ability to restore deleted files previously uploaded, and recover file versions previously uploaded.

Data Redundancy

The Data Processor employs multiple layers of data redundancy to guard against data loss and ensure availability.

Data Centers and Location

The Data Processor's production systems are housed at multiple co-location data centers in Toronto, ON Canada. Canada provides an adequate level of data protection as required by Art 45 (1) GDPR. The Data Processor periodically reviews the data center's Service Organization Control (SOC) reports, SOC 1 and/or SOC 2, for sufficient security controls.

Confidentiality

The Data Processor treats all the Personal Data transferred by the Data Controller as strictly confidential information. Access to the Personal Data is restricted to only the employees to whom it is necessary and relevant to process the Personal Data in order for the Data Processor to perform its obligations under the Main Agreement and this Data Processor Addendum. The Data Processor's employees are subject to background checks and non-disclosure agreements, as well as ongoing training on policies and procedures.

Change Management
The Data Processor ensures that all security-related changes have been authorized by the appropriate level of management prior to implementation.

6 - Engagement of further processors

6.1 - The Controller hereby authorizes the Processor to engage further processors in a general manner.

6.2 - The following sub-processors shall be considered approved by the Data Controller at the time of entering into this Data Processing Agreement for billing purposes and payment processing (Paypal, U.S., Bitpay, U.S., Zuora Inc., U.S.), for sales and technical support (Helpscout, U.S., Slack Technologies Inc., U.S.), for transactional email communications (SendGrid, U.S., MailJet, U.S.), and for marketing communications (MailChimp, U.S.).

The Data Processor requires that these processors also comply with the GDPR and the applicable data protection laws. These subprocessors are prohibited from using the Data Controller's Personal Data for any purposes other than as stipulated in the Terms of Use.

6.3 - The Processor shall inform the Controller of any intended changes concerning the addition or replacement of further processors. The Controller is entitled to object to any intended change. If the Controller objects, the Processor is prohibited from making the intended change. In the event of authorised modifications, the Processor shall update this agreement accordingly and make it available to the Controller.

6.4 - The Processor shall contractually impose the same data protection obligations on each further processor as set out in this Addendum with respect to the Processor.

6.5 - The Processor shall monitor that appropriate technical and organisational measures have been taken by the further processors and that the measures are carried out in such a way that the processing of Controller Data is carried out in accordance with this Addendum.

7 - Support obligations of the Processor

7.1 - The Processor shall to a reasonable extent support the Controller with technical and organisational measures in fulfilling his obligation to respond to requests for exercising data subjects' rights.

7.2 - The Processor shall notify the Controller immediately after becoming aware of any breach of Controller Data, in particular any incidents that lead to the destruction, loss, alteration or unauthorized disclosure of or access to Controller Data. If possible, the notification shall contain a description of:

- the nature of the breach of Controller Data, indicating, as far as possible, the categories and the approximate number of affected data subjects, the categories and the approximate number of affected personal data sets;
- the likely consequences of the breach of Controller Data;
- the measures taken or proposed by the Processor to remedy the breach of Controller Data and, where appropriate, measures to mitigate their potential adverse effects.

7.3 - In the event that the Controller is obligated to inform the supervisory authorities and/or data subjects in accordance with Art. 33, 34 of GDPR, the Processor shall, at the request of the Controller, assist the Controller to comply with these obligations.

7.4 - The Processor shall to a reasonable extent assist the Controller with data protection impact assessments to be carried out by him and, if necessary, subsequent consultations with the supervisory authority pursuant to Art. 35, 36 GDPR if applicable.

8 - Deletion and return of Controller Data

Upon the instruction of the Controller, the Processor shall, upon termination of the Terms of Use completely and irrevocably delete all Controller Data, unless the Processor is obligated by law to further store Controller Data.

9 - Evidence and audits

9.1 - The Processor shall ensure and regularly control that the processing of Controller Data is consistent with this Addendum and with the instructions of the Controller.
9.2 - The Processor shall document the implementations of the obligations under this Addendum in an appropriate manner and provide the Controller with appropriate evidence at the latter´s request.

9.3 - Upon request prior to the start of processing of Controller Data and regularly – however not more often than annually - during the term of the Terms of Use, the Processor shall make available to the Controller all information necessary to demonstrate their compliance with the provisions of this Addendum, in particular the implementation and organizational measures as defined in Section 5.

Executed by the Parties’ authorized signatories:

Date	
Legal Name	**Sync.com Inc.** Legal Name
Signature	Signature
Title	**CEO** Title
City, Province, Country	**Toronto Ontario, Canada** Location

*Your typed signature and submission of the document constitutes a legal and binding signature to the DPA with Sync.com, Inc.