Data Processing Addendum

This Data Processing Addendum, ("***Addendum***" or "***DPA***"), by and between **Customer** ("***Company***"), and **Together (US) Inc.**, a corporation registered in the state of Delaware ("***Together***" or ***Service Provider***") (collectively referred to as the ***"Parties"***), sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Service Provider to Company pursuant to the **Master Software Services Agreement** with Together (the "***Master Agreement***").

Whereas, Company or its employees, agents, consultants or contractors (collectively, "***Company Personnel***") shall provide Service Provider with access to Personal Data in connection with certain services performed by Service Provider for or on behalf of Company pursuant to the Master Agreement; and

Whereas, Company requires that Service Provider preserve and maintain the privacy, confidentiality and security of such Personal Data.

(1) Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Master Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Company and Service Provider agree as follows:

I. Definitions

(A) ***"Applicable Law"*** means all applicable legislation, laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the EU General Data Protection Regulation 2016/679 ("GDPR"), EU Member State laws supplementing the GDPR, the GDPR as incorporated into UK law ("UK GDPR"), the UK Data Protection Act 2018, the EU Directive 2002/58/EC ("e-Privacy Directive"), and UK and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications, and the Personal Information Protection Law of the People's Republic of China ("PIPL"), each as replaced from time to time,.

(B) ***"Chinese SCCs"*** has the meaning given in Section IV.C.

(C) "***Data Controller***" means the entity that determines the purposes and means of the Processing of Personal Data and includes, for purposes of the PIPL a "**Personal Information Processor**".

(D) "***Data Processor***" means any person or entity that Processes Personal Data on behalf of the Data Controller and includes, for purposes of the PIPL, an "**Entrusted Party**".

(E) ***"Data Security Measures"*** means technical and organizational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.

(F) ***"Data Subject"*** means an identified or identifiable natural person to which the Personal Data pertain.

(G) ***"Instructions"*** means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

(H) ***"Personal Data***" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular identified or identifiable individual or household, regardless of the media in which it is maintained, that may be: (i) disclosed at any time to Service Provider or Service Provider personnel, by or on behalf of Company in anticipation of, in connection with or incidental to the performance of services for or on behalf of Company; (ii) Processed at any time by Service Provider or Service Provider personnel in connection with or incidental to the performance of this Addendum or the Master Agreement, or (iii) derived by Service Provider or Service Provider personnel from the information described in (i) or (ii) above.

(I) **"*Personal Data Breach***" means any actual or suspected breach of security leading to unauthorized or accidental access to or loss, use, disclosure, modification, destruction, acquisition or Processing of any Personal Data.

(J) "***Process***", "***Processed***", and "***Processing***" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, including, without limitation, creating, collecting, aggregating, procuring, obtaining, accessing, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, transferring, transmitting, providing, disclosing, disseminating, making available, aligning, combining, restricting, erasing, deleting and/or destroying the information.

(K) ***"Request(s)"*** means a subpoena, warrant or other judicial, regulatory, governmental or administrative order, proceeding, demand or request (whether formal or informal) by a non-EEA or UK government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) (a ***"Government Authority"***) seeking or requiring access to or disclosure of Personal Data;

(L) ***"Sub-Processor"*** means the entity engaged by the Data Processor or any further Sub-Processor to Process Personal Data on behalf and under the authority of the Data Controller.

(M) ***"Transfer Clauses*"** means: (i) the EU Commission standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as attached at Annex 2 ("***EU SCCs***"); and (ii) the International Data Transfer Addendum to the EU SCCs, version B1.0, in force 21 March 2022, attached at Annex 3 ("***UK Addendum***").

II. Roles and Responsibilities of the Parties

(A) The Parties acknowledge and agree that Company is acting as a Data Controller, and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this Addendum, and Service Provider is acting as a Data Processor on behalf and under the Instructions of Company.

III. Obligation of the Service Provider

Service Provider agrees and warrants to:

(A) process Personal Data disclosed to it by Company only on behalf of and in accordance with the Instructions of the Data Controller and Annex 1, unless Service Provider is otherwise required by Applicable Law, in which case Service Provider shall inform Company of that legal requirement before Processing the Personal Data, unless informing the Company is prohibited by law on important grounds of public interest. Service Provider shall immediately inform Company if, in Service Provider's opinion, an Instruction provided infringes Applicable Law;

(B) ensure that any person authorized by Service Provider to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Company;

(C) inform Company promptly and without undue delay of any formal requests from Data Subjects exercising their rights under Applicable Law including, as applicable, their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by the Company in writing to do so. Taking into account the nature of the Processing of Personal Data, Service Provider shall assist Company, by appropriate technical and organizational measures, insofar as possible, in fulfilling Company's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data; and

(D) assist Company in complying with its obligations under Applicable Law, in particular Company's obligation to implement appropriate Data Security Measures, to carry out a data protection impact assessment, and to consult the competent supervisory authority.

IV. Data Transfers

(A) The Parties shall comply with (i) the terms of the EU SCCs in relation to Personal Data the processing of which is subject to the GDPR, and (ii) the terms of the UK Addendum in relation to Personal Data the processing of which is subject to the UK GDPR.

(B) Other than in respect of transfers of Personal Data to any of the Sub-processers listed in Annex 1 to the DPA, Service Provider shall not transfer Personal Data to any person in a country located outside the EEA, the UK or Switzerland without the explicit written consent of Company. In relation to any such transfer of Personal Data authorized by Company, Service Provider shall, as a condition to carrying out such transfer, procure that the recipient of such Personal Data outside of the UK, EEA or Switzerland shall enter into the relevant Transfer

Clauses with Service Provider (or such other Standard Contractual Clauses that are available under Applicable law, a copy of which shall be provided by Service Provider to Company promptly upon request), unless the recipient is located in a country which has been deemed adequate in accordance with Applicable Law or has otherwise implemented or adopted an appropriate transfer mechanism in accordance with Applicable Law, including Binding Corporate Rules for Data Processors.

(C) If Personal Data, the processing of which is subject to PIPL, is transferred to a Party outside of China, the Parties agree to execute the standard contractual clauses approved by the Cyberspace Administration of China or other appropriate Governmental Authority in China (the "**Chinese SCCs**") and comply with all other applicable requirements under PIPL to lawfully transfer the relevant Personal Data. Until such time as the Chinese SCCs are executed, if any Personal Data, the processing of which is subject to PIPL, is transferred to a Party outside of China, the recipient of the Personal Data shall process the Personal Data in a secure manner and in accordance with the terms of this Addendum, and provide the Personal Data a standard of data protection substantially similar to that provided by PIPL.

V. Sub-Processing

(A) Service Provider shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless Company has authorized Service Provider to do so in writing. Where Service Provider, with the consent of Company, provides access to Personal Data to a third party, Service Provider shall enter into a written agreement with each such third party that imposes obligations on the third party that are the same as those imposed on Service Provider under this Addendum. Service Provider shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data.

VI. Compliance with Applicable Laws

(A) Service Provider shall comply with all Applicable Laws.

(B) Service Provider shall enter into any further data Processing agreement reasonably requested by Company for purposes of compliance with the Applicable Law. In case of any conflict between this Addendum and the Master Agreement, this Addendum shall prevail with regard to the Processing of Personal Data covered by it.

VII. Data Security

(A) Service Provider shall develop, maintain and implement a comprehensive written information security program that shall include appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

(1) The pseudonymization and encryption of the Personal Data;

(2) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(3) The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and

(4) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures adopted pursuant to this provision for ensuring the security of the Processing.

(B) Promptly upon the expiration or earlier termination of the Master Agreement, or such earlier time as Company requests, Service Provider shall return to Company or its designee, or at Company's request, securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Service Provider's, its affiliates' or their respective subcontractors' possession, custody or control. In the event applicable law does not permit Service Provider to comply with the delivery or destruction of the Personal Data, Service Provider warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.

VIII. Data Breach Notification

(A) Service Provider shall immediately inform Company in writing of any Personal Data Breach of which Service Provider becomes aware, but in no case longer than twenty four (24) hours after it becomes aware of the Personal Data Breach. The notification to Company shall include all available information regarding such Personal Data Breach, including information on:

a.

(2) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;

(3) The likely consequences of the Personal Data Breach; and

(4) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

(B) Service Provider shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Company in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. Service Provider shall provide such assistance as required to enable Company to satisfy Company's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR. The content of any filings, communications, notices, press releases or reports related to any Personal Data Breach must be approved by Company prior to any publication or communication thereof. Service Provider shall be responsible for the costs and expenses associated with the performance of its obligations described in this paragraph, unless the Personal Data Breach is caused by the acts or omissions of Company or its affiliates.

a

IX. Additional Contractual Safeguards for Data Transfers

(A) Prior to Processing Personal Data, Service Provider shall undertake a detailed assessment to consider whether, having regard to the nature of the Personal Data, the purposes and context of the Processing, and the country of destination, it is able to ensure an adequate level of protection for the Personal Data as required by Applicable Law. As part of this assessment, Service Provider shall consider what additional safeguards may be implemented to ensure an adequate level of protection for the Personal Data it Processes. Service Provider shall document this assessment, including any additional safeguards implemented, and make it available to Company upon request.

(B) Service Provider shall implement, maintain and comply with a documented procedure for reviewing and responding to Requests. Such procedure shall require Service Provider to:

a. Upon receipt of a Request, and to the extent permitted by law, notify Company in writing of any such Request, and cooperate with Company in responding to any such request;

b. Reject or contest any request that is not valid, legally binding and lawful;

c. Ensure that the Personal Data made available in response to a Request or to which access is provided, is proportionate and limited to the minimum amount that is strictly necessary for the purpose of complying with the Request; and

d. Perform reasonable due diligence on, and obtain appropriate written assurances from, each Sub-processor that Processes Personal Data to ensure that each Sub-processor has adopted adequate safeguards to protect Personal Data in connection with Requests.

(C) Where Service Provider anticipates or receives a Request concerning Personal Data provided by Company (or any portion thereof), Service Provider shall:

b

a. In advance of providing any response or making any disclosure, notify Company in writing of such Request so that Company may, or require Service Provider to, contest or seek to narrow such disclosure or seek a protective order or other appropriate remedy. Where permitted by law, Service Provider shall seek to redirect the Government Authority (or other third party) to request the Personal Data directly from Company;

b. To the fullest extent permitted by law, fully cooperate with and take all reasonable steps to assist Company to contest or seek to narrow such Request, obtain a protective order or seek another remedy at Company's discretion; and

c. To the fullest extent permitted by law, ensure that it does not provide any Government Authority (such as law enforcement or intelligence agencies) public or private cryptographic keys used to secure Personal Data or the ability to break such encryption.

(D) Service Provider shall maintain a written record of all Requests that, to the extent permitted by law, includes (i) the government authorities making the Request, (ii) the number of Requests received and how Service Provider responded to such Requests, (iii) the types of Personal Data provided in response to a Request, and (iv) the number of Data Subjects whose Personal Data was made available in response to a Request. To the extent permitted by law, Service Provider shall make aggregated information from such records available to Company upon request.

(E) Service Provider shall implement appropriate technical and organizational safeguards to protect Personal Data in transit over public networks between Company and Service Provider (and any applicable Sub-processors), including by ensuring that all Personal Data is encrypted by default and that, to the extent possible, the applicable decryption key(s) shall be stored in the EU or the UK.

X. Audit

Service Provider shall make available to Company all information necessary to demonstrate compliance with the obligations set forth in this Addendum and to allow Company to supervise Service Provider's Processing, and allow for and contribute to audits, including inspections, conducted by Company or another auditor mandated by Company.

IN WITNESS WHEREOF, the parties acknowledge their agreement to the foregoing by due execution of the Addendum by their respective authorized representatives.

ANNEX 1 TO THE DPA

SCOPE OF THE DATA PROCESSING

SCOPE OF THE DATA PROCESSING

This Annex forms part of the Data Processing Addendum between Company and Service Provider.

The Processing of Personal Data concerns the following categories of Data Subjects:

Exporter Employees

The Processing concerns the following categories of Personal Data:

Contact Information (Name, Email)
Employment Information (Job Title, Department, Office)

The Processing concerns the following categories of Sensitive Data:

Sensitive Data shall have the meaning ascribed to it under Applicable Law and may include Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation, government-issued identifiers, financial account information, precise geolocation data, or other Personal Data that, if subject to an actual Personal Data Breach, could result in harm to relevant Data Subjects.

Data such as:

Racial or ethnic origin
Gender
Sexual orientation

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):

The purpose of the processing by Service Provider is the performance of the services under the Master Agreement. Such processing includes collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, review, consultation, use, access, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Service Provider uses the following Sub-Processors:

See Annex III

ANNEX 2 TO THE DPA: EU SCCs

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(b) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex

II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(e) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) Data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 14 working days prior to the engagement of the subprocessor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<u>SECTION IV – FINAL PROVISIONS</u>

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Luxembourg.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts where of Luxembourg.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO ANNEX 2

ANNEX I TO THE SCCS

A. LIST OF PARTIES

By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses.

Data exporter(s):

Name: Company

Address: Company address on Order Form

Contact person's name, position and contact details: Company contact on Order Form

Activities relevant to the data transferred under these Clauses: The performance of the Master Agreement.

Signature and date: Signature of this DPA shall be deemed signature of the EU SCCs.

Role: Controller

Data importer(s):

Name: Together (US) Inc.

Address: 251 Little Falls Drive, Wilmington, DE 19808

Contact person's name, position and contact details: Matthew Reeves, Director, matthew@togetherplatform.com

Activities relevant to the data transferred under these Clauses: The performance of the Master Agreement.

Signature and date: Signature of this DPA shall be deemed signature of the EU SCCs.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

See Annex 1 of the DPA.

Categories of personal data transferred:

See Annex 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Annex 1 of the DPA.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):

The personal data will be transferred on a continual basis for the duration of the Master Agreement.

Nature of the processing:

Collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, review, consultation, use, access, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing:

The personal data will be transferred to and processed by the Service Provider to perform the services under the Master Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

Personal data will be retained by Service Provider for the duration of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

See Annex 1 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The Luxembourg National Commission for Data Protection (*Commission Nationale pour la Protection des Données*)

ANNEX II TO THE SCCS - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data	● Pseudonymization, where possible; ● Encryption at rest and encryption in transit; ● Encryption key kept in the EU or with a trusted third party; ● Limited timespan for using personal data "in the clear" (i.e., in identifiable form);
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	● Confidentiality arrangements; ● Information security policies and procedures; ● Backup procedures; ● Remote storage; ● Mirroring of hard disks (e.g., RAID technology); ● Uninterruptible power supply; ● Anti-virus/firewall protection, security patch management; ● Intrusion prevention, monitoring and detection; ● Availability controls to protect personal data against accidental destruction or loss;
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	● Business continuity plan; ● Disaster recovery procedure; ● Incident response plan;
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	● Internal and external audit program, audit reports and documentation; ● Testing of back up processes and business continuity procedures; ● Risk evaluation and system monitoring on a regular basis; ● Vulnerability and penetration testing on a regular basis;

Measures for user identification and authorisation	● Internal policies and procedures; ● User authentication controls, including secure methods of assigning selecting and storing access credentials and blocking access after a reasonable number of failed authentication access; ● Restricting access to certain users; ● Access granted based on a need-to-know, supported by protocols for access authorization, establishment, modification and termination of access rights; ● Logging and reporting systems; ● Control authorization schemes; ● Differentiated access rights (profiles, roles, transactions and objects); ● Monitoring and logging of accesses; ● Disciplinary action against employees who access personal data without authorization; ● Reports of access; ● Access procedure; ● Change procedure;
Measures for the protection of data during transmission	● Encryption in transit; ● Pseudonymization, where possible; ● Transport security; ● Network segregation; ● Logging; ● Electronic signatures;
Measures for the protection of data during storage	● Encryption at rest; ● Access controls; ● Separation of databases and logical segmentation of Company personal data from data of other vendor customers; ● "Internal client" concept / limitation of use; ● Segregation of functions (production/testing); ● Procedures for storage, amendment, deletion, transmission of data for different purposes; ● Process Personal Data in multiple separate locations or by using multiple parties;
Measures for ensuring physical security of locations at which personal data are processed	● Establishing security areas, restriction of access paths;

	● Establishing access authorizations for employees and third parties with a need-to-know; ● Access control system (ID reader, magnetic card, chip card); ● Key management, card-keys procedures; ● Door locking (electric door openers etc.); ● Security staff, janitors; ● Surveillance facilities, video/CCTV monitor, alarm system; ● Securing decentralized processing equipment and personal computers;
Measures for ensuring events logging	● User identification and authentication procedures; ● ID/password security procedures (special characters, minimum length, change of password); ● Automatic blocking (e.g., password or timeout); ● Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; ● Creation of one master record per user; ● Encryption and pseudonymization;
Measures for ensuring system configuration, including default configuration	● Up-to-date baseline configuration documentation and settings;
Measures for internal IT and IT security governance and management	● Information security policies and procedures; ● Incident response plan; ● Regular internal and external audit: ● Review and supervision of information security program;
Measures for certification/assurance of processes and products	● SOC II
Measures for ensuring data minimisation	● Documentation regarding which data categories need to be processed; ● Ensure that the minimum amount of data is processed to fulfill the purpose of the processing;

	● Personal data is stored in the EU and only remote access or view-only access is enabled;
Measures for ensuring data quality	● Personal data is kept accurate and up to date; ● Data is corrected upon request or where necessary;
Measures for ensuring limited data retention	● Records retention schedule; ● Data retention policy; ● Personal data is deleted or irreversibly anonymized after expiration of the retention period;
Measures for ensuring accountability	● Internal policies and procedures; ● Privacy by design and by default; ● Records of data processing activities; ● Privacy Impact Assessments, where required; ● Adequate agreements with third parties; ● Criteria for selecting the sub-processors; ● Vendor onboarding process and questionnaire; ● Monitoring of contract performance; ● GDPR and InfoSec training program;
Measures for allowing data portability and ensuring erasure	● Personal data in made available upon request in an electronically portable format using industry standards; ● Reduction methods are used, where necessary; ● Secure disposal of information stored on magnetic and non-magnetic media that prevents potential recovery of the information;

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter:

Risk Management Program

Together will maintain a risk management program that aligns to ISO 27005 or NIST 800-37. This should include at a minimum:

- Annual risk reviews
- SOC II – Together should provide up-to-date SOC II reports to Company, as and when requested by Company
- Documentation on risk decisions

- Senior leadership approval of risk mitigations and acceptance

Information Security Requirements
Together will maintain reasonable operating standards and security procedures and use best efforts to secure the Controller data through the use of appropriate physical and logical security measures including, but not limited to, appropriate network security and encryption technologies. Together will use reasonable user identification or password control requirements and other security procedures, as may be issued from time to time by the Controller in relation to the Controller data.

Information Security Policies – Together will maintain a documented set of rules and procedures regulating the use of information, including its receipt, transmission, processing, storage, control, distribution, retrieval, access and presentation. This includes the laws, rules and practices that regulate how an organization manages, protects, and distributes confidential information.

Encryption – The Controller's data must be encrypted while in transit on any network or stored on any device. Use of encryption products must comply with local restrictions and regulations on the use of encryption in a relevant jurisdiction.

Logical Access Control – Together must ensure authentication and authorization controls are appropriately robust for the risk of the data, application and platform. Together will monitor access rights to ensure they are the minimum required for the current business needs of the users but not more than required. Access and security events will be logged and software deployed that enables rapid analysis of user activities.

- Password Policy – Together must maintain and enforce a password policy for systems maintaining and/or accessing the Controller data that requires
  - Forced or initial password change
  - Minimum password length
  - Password complexity
  - Password history
  - Password must not be shared
- Together must maintain procedures for inactivating accounts and removing users after allowed thresholds.
- Together will require multi-factor authentication for remote access

Cloud File Sharing - The Controller's data and reports will be transferred by using only the Controller's authorized file transfer repositories.

Security Controls – Together agrees to maintain the minimum security controls:

- Endpoint security software on all workstations and servers (i.e., anti-malware)
- Anti-spam filters
- Perimeter firewalls
- Logical access controls
- Logging of access to all the Controller data

- Intrusion Prevention and/or Detection Systems
- Security Event and Information Management

Vulnerability Scanning and Patching – Together agrees to:

- Conduct daily internal and external vulnerability scans
- Conduct annual external penetration tests
- Correct critical findings from vulnerability scans and penetration tests within 30 days
- Apply critical patches within 30 days.

Third Party Relationships/Sub-processors – Together must have a process to review all third party service providers and sub-processors security policies and procedures and ensure that appropriate security language is incorporated into all third party service provider and sub-processor agreements. Together must ensure that the Controller is aware of any subcontracting or outsourcing, that any required approval is obtained, and that any required due diligence is completed. Controller data may not be provided to a third party vendor (subcontractor) without Controller consent.

Breach Notification – If you learn, or have reason to believe, that any person or entity has breached or attempted to breach your security measures, or gained unauthorized access to the Controller data, you will immediately notify the Controller's Information Security Team within 48 hours. Consequently, you must investigate, remediate, and mitigate the effect of the information security breach. Such cooperation will include but is not limited to cooperating with the Controller's Information Security Team, and providing assurances reasonably satisfactory to us that such an information security breach will not recur. If to the extent any information security breach or other unauthorized access, acquisition or disclosure or personal information occurs as a result of Together's act or omission, Together agrees to provide the following at Together's expense upon the Controller's request:

a) notice to individuals whose Personal Data was affected by the Security Incident in a manner and format determined by the Controller, in its sole discretion, as well as to any other third parties, such as Regulators, law enforcement agencies and consumer reporting agencies, that the Controller determines should be notified of the Security Incident, in its sole discretion;

b) one year of credit monitoring;

c) any other relief service(s) as required by applicable law to affected individuals; and

d) reasonable co-operation with the Controller to offer any other remediation services deemed necessary by the Controller or which are customarily provided to individuals impacted by a breach in confidentiality of their Personal Data in the relevant jurisdictions.

Insurance – Together will maintain cyber security insurance of a minimum amount of 2 million USD.

ANNEX III TO THE SCCS – LIST OF SUBPROCESSORS

The controller has authorized the use of the following sub-processors:

Company name	Country of Processing	Description of the processing	Transfer Mechanism
Amazon Web Services, Inc. 410 Terry Avenue North, Seattle, WA 98109-5210 U.S.A.	As per client selected hosting region	Storage and services	SCCs-
Mailgun Technologies, Inc 112- E. Peca-n Stre-et #113-5, San- Anto-nio, Texa-s, 7820-5 USA MG-privacy@sinch.com	United States of America	Transactional email server	SCCs-
Amplitude, Inc 201 3rd Street, Suite 200 San Francisco, CA 94103 United States privacy@amplitude.com	United States of America	Product analytics	SCCs-
Functional Software, Inc. d/b/a Sentry 45 Fremont Street, 8th Floor, San Francisco, CA 94105 legal@sentry.io	United States of America	Product analytics	SCCs-
OpenAI OpCo, LLC 3180 18th St. San Francisco, CA 94110 privacy@openai.com	United States of America	Generative AI	SCCs-
Together Software Inc. (Subsidiary of Together (US) Inc.) 325 Front St. W Toronto, ON M5V 2Y1 Canada legal@togetherplatform.com	Canada	Customer Support	Adequate regulations

Hotjar Ltd Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta	EU	Product analytics	SCCs
Intercom, Inc.	United States of America	Leveraging Fin.ai to enable automated customer service resolution, improve response accuracy and speed, analyze support trends, and optimize customer support	SCCs-
Absorb Software Inc. and its affiliates and subsidiaries	Canada, USA, UK, EU, Australia	Support and technical services as applicable	Intercompany agreements