

Data Processing Agreement

Updated May 11, 2026

This Data Processing Agreement (this “**DPA**”) forms a part of the [Terms of Use](#) (the “**Agreement**”) entered into by and between DSOA and you. Any capitalized terms used in this DPA but not defined shall have the respective meanings given to them in the Agreement. The Parties enter into this DPA to comply with applicable Data Protection Laws (as defined below). The Parties agree that the processing of Personal Data (as defined below) under or in connection with the Agreement shall be in accordance with this DPA, including all Annexes to this DPA.

You agree that you are entering into this DPA on behalf of yourself and, to the extent required under Applicable Law, in the name and on behalf of your Authorized Affiliates (as defined below), if and to the extent DSOA processes Personal Data for which such Authorized Affiliates qualify as the “controller”. For the purposes of this DPA only, and except as indicated otherwise, the term “you” shall include you and your Authorized Affiliates.

1. DEFINITIONS.

- 1.1 “**Audit**” means requests, audits, and/or inspections, the scope of which shall be mutually agreed upon by the Parties in advance, relating to the processing of Your Personal Data by DSOA or any Sub-processor, in each case to enable you to verify DSOA’s compliance with this DPA and Data Protection Laws.
- 1.2 “**Authorized Affiliates**” means any of your affiliate(s) which (a) is subject to the Applicable Laws of the European Union, the European Economic Area and/or their member states, and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between you and DSOA, but has not entered into its own agreement with DSOA.
- 1.3 “**Data Protection Authority**” means a legislative, executive, administrative, or regulatory entity, judicial body, or other public agency or authority of any country, state, territory, or political subdivision thereof, or a person or entity acting under a grant of authority from or under contract with such public agency or authority, that is authorized by law to enforce, or to oversee or monitor compliance with, Data Protection Laws.
- 1.4 “**Data Protection Laws**” means all laws and regulations relating to or impacting the processing, privacy, or security of Personal Data, in each case as may be amended or replaced from time to time, including: (a) the GDPR; (b) any national law of an EU member state adopted pursuant to the GDPR; (c) the Switzerland Federal Act on Data Protection; (d) the United Kingdom Data Protection Act of 2018; and (d) State Data Protection Laws.
- 1.5 “**Data Subject**” means an individual whose Personal Data is collected, processed, or stored.
- 1.6 “**EU**” means the member states, at any given time, that make up the European Union.
- 1.7 “**GDPR**” means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- 1.8 “**Personal Data**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to, a natural person, including information that meets the definition of “Personal Data,” “personal data,” “personally identifiable information,” “sensitive Personal Data” or similar term under applicable Data Protection Laws.
- 1.9 “**Personal Data Breach**” means any actual or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- 1.10 “**Security Schedule**” means Annex 2 (Security Schedule) of this DPA.
- 1.11 “**State Data Protection Laws**” means the California Consumer Privacy Act (Cal. Civ. Code 1798.100 et. seq.) (“**CCPA**”), as amended by the California Privacy Rights Act (“**CPRA**”), the Virginia Consumer Data Privacy Act (Va. Code Ann. § 59.1-571 et. seq.) (“**CDPA**”), and the Colorado Privacy Act (Colo. Rev. Stat. § 6-1-1301 et. seq.) (“**CPA**”).
- 1.12 “**Sub-processor**” means any third-party appointed by DSOA to process Personal Data on behalf of DSOA in connection with the Agreement.
- 1.13 “**Your Personal Data**” means any Personal Data: (i) supplied by or on behalf of you to DSOA (including where DSOA has access to Personal Data held by DSOA or on DSOA’s behalf), or which DSOA collects or generates on your behalf; (ii) that is processed by DSOA under or in connection with the Agreement as further described in Clause 2.2(a) of this DPA; and (iii) in respect of which you are a controller or owner (or equivalent).

2. DATA PROCESSING

2.1 Status of Each Party under Data Protection Laws

You and DSOA acknowledge that the status of each Party is a question of fact determined under Data Protection Laws. Without limiting the foregoing, you and DSOA each understand that, in relation to the Personal Data processed under the Agreement,

you are the controller (or “business” as defined by the CCPA and CPRA) and DSOA is the processor (or “service provider” as defined by the CCPA and CPRA) of Your Personal Data and all processing of Your Personal Data by DSOA shall be undertaken in accordance with Annex 1 (Data Processor Terms). You shall have sole responsibility for the accuracy, quality, and legality of Your Personal Data and the means by which you acquired Your Personal Data.

2.2 Description of Processing

(a) All processing of Your Personal Data undertaken by DSOA is described in this Clause 2.2(a).

Duration, nature and purpose of processing	
Duration of processing	Unless stated otherwise in the Agreement, or agreed to in writing between the Parties, Personal Data will be processed for the term of the Agreement, and any such additional period stated in the Agreement.
Nature and purpose of processing	For the purpose of the provision of Services by DSOA under the Agreement.
Personal Data	
Individuals may include any of:	As directed by you in connection with your use of the Services.
Categories of Personal Data may include any of:	As directed by you in connection with your use of the Services.
Special categories of Personal Data may include any of:	As directed by you in connection with your use of the Services.

3. INTERNATIONAL DATA TRANSFERS

(a) For purposes of this DPA, “**Standard Contractual Clauses**” means the Standard Contractual Clauses set out in Decision (EU) 2021/915 with the Clauses corresponding to module two (controller to processor) selected and “**UK Addendum**” means the addendum to the Standard Contractual Clauses issues pursuant to Section 119A of the United Kingdom Data Protection Act. You (as data exporter) and DSOA (as data importer) shall comply with the Standard Contractual Clauses with respect to Personal Data exported from the European Economic Area to the United States of America or other third country that has not been deemed by the European Commission to ensure an adequate level of protection for such Personal Data. The Standard Contractual Clauses and UK Addendum are hereby incorporated into this DPA by this reference, with the following information deemed selected and prepopulated:

- (i) Option 2 of Clause 9(a) of the Standard Contractual Clauses, “general written authorization,” is deemed to be selected, with DSOA to inform you in writing of any addition or replacement of Sub-processors at least fourteen (14) days in advance.
- (ii) Clause 7 shall be deemed incorporated into the Standard Contractual Clauses.
- (iii) Option 1 of Clause 17 of the Standard Contractual Clauses is deemed to be selected, with Irish law deemed to be selected for purposes of such Clause.
- (iv) Clause 18(b) of the Standard Contractual Clauses is deemed to be prepopulated with “courts of Ireland”.
- (v) Annex I.A of the Standard Contractual Clauses is deemed to be prepopulated as follows: (a) the identity and the contact details of the data exporter are deemed to be prepopulated with the name and address you have provided to DSOA when you initiated the Services, the “Contact person’s name, position and contact details” is deemed to be you or the administrator for your account, as applicable, the “Activities relevant to the data transferred under these Clauses” is deemed to be the provision of the Services as set forth in the Agreement, the “Role” is deemed to state “controller”, and your duly authorized representative is deemed to have signed and dated Annex I.A as of the effective date of the Agreement; and (b) the identity and the contact details of the data importer are deemed to be prepopulated with the name and address of DSOA as specified in the Agreement, the “Contact person’s name, position and contact details” is deemed to be Damon E. Schramm, Chief Legal Officer, legal@togetherwork.com, the “Activities relevant to the data transferred under these Clauses” is deemed to be the provision of the Services as set forth in the Agreement, the “Role” is deemed to state “processor”, and DSOA’s duly authorized representative is deemed to have signed and dated Annex I.A as of the effective date of the Agreement.
- (vi) Annex I.B of the Standard Contractual Clauses is deemed to be prepopulated with the information specified the relevant sections of Section 2.2 of this DPA.
- (vii) Annex I.C is deemed to be prepopulated with the Irish Data Protection Commission.
- (viii) Annex II is deemed to be prepopulated with the technical and organizational measures specified in the Security Schedule.

- (ix) All other optional clauses are deemed not to be included in the Standard Contractual Clauses.
- (b) With respect to Personal Data of any Data Subject in the United Kingdom exported from the United Kingdom to the United States or any other third country that has not been deemed by the United Kingdom to ensure an adequate level of protection for such Personal Data, (i) the Standard Contractual Clauses shall apply to such transfers as provided in Section 3(a) above, (ii) the UK Addendum shall be deemed executed between the Parties, and (iii) the Standard Contractual Clauses shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Personal Data from the United Kingdom to countries that have not been the subject of an adequacy decision.
- (c) Where any mechanism for international transfers of Personal Data ceases for any reason to be a valid means of complying with the restrictions on transferring Personal Data to a third country as set out in Data Protection Laws, or otherwise ceases to apply for any reason, the Parties shall act in good faith to agree the implementation of an alternative solution to enable both Parties to comply with Data Protection Laws.

4. **AUTHORIZED AFFILIATES**

- (a) **Contractual Relationship.** The Parties acknowledge and agree that, by entering into this DPA, you enter into this DPA on behalf of yourself and, as applicable, in the name and on behalf of your Authorized Affiliates, thereby establishing a separate DPA between DSOA and each such Authorized Affiliate subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of this DPA and the Agreement and any breach of the terms and conditions of this DPA or the Agreement by an Authorized Affiliate shall be deemed a breach by you.
- (b) **Communication.** You as the contracting party to the Agreement shall remain responsible for coordinating all communication with DSOA under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of your Authorized Affiliates.
- (c) **Rights of Authorized Affiliates.** Except where Applicable Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against DSOA directly by itself, the Parties agree that solely you as the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of any Authorized Affiliate, including any rights or remedies under this DPA, in each case, not separately for each Authorized Affiliate individually but in a combined manner for all of your Authorized Affiliates together.

5. **YOUR OBLIGATIONS**

- (a) As controller, you represent and warrant that: (i) Applicable Laws do not prevent DSOA from fulfilling your instructions and performing DSOA's obligations under this DPA; (ii) you have complied and will continue to comply with Applicable Laws regarding the processing of Personal Data under the Agreement; and (iii) you have obtained any necessary consents or given any required notices, and otherwise have a legitimate ground to disclose the Personal Data to DSOA and enable the processing of the Personal Data by DSOA as set out in this DPA and as contemplated by the Agreement.
- (b) You also warrant that you maintain accurate and up to date records of your legal basis for processing, including relevant consent flows. If you are relying on "legitimate interest" under Article 6(1)(f) of the GDPR, you warrant that you have balanced your interests against the fundamental rights of the Data Subject and keep records of this process.
- (c) You agree that you will jointly and severally together with any other controller, indemnify and hold harmless DSOA, its affiliates, and their respective officers, directors, employees, and agents, on demand from and against all losses, damages, liabilities, penalties, costs, and expenses (including reasonable attorney's fees) arising from any third-party claim, suit, action, or proceeding relating directly or indirectly from your breach of this Clause.

6. **LIMITATIONS OF LIABILITY**

- (a) Each Party's and all of its affiliates' total liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and DSOA, whether in contract, tort, or under any other theory of liability, is subject to the limitations of liability and disclaimers in the Agreement, including any 'Limitations of Liability' section (however described) of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its affiliates under the Agreement and all DPAs together.
- (b) For the avoidance of doubt, DSOA's total liability for all claims from you and all of your Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established hereunder, including by you and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to you and/or to any Authorized Affiliate that is a contractual party to any such DPA.

7. SEVERANCE

Should any provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (1) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (2) constructed in a manner as if the invalid or unenforceable part had never been contained therein.

8. CHANGES

DSOA may update this DPA at any time by posting an updated version online; provided, however, if there is any material update to how DSOA plans to process your Personal Data under the Agreement, such changes will not take effect until thirty (30) days following the posting of the updated terms. During such thirty (30) day period, you have the opportunity to object to any such changes by notifying DSOA in writing. The Parties may either execute a written amendment to the Agreement implementing any agreed upon changes, or you may exercise your right to terminate the Agreement in accordance with the termination provisions thereof. Such termination shall not constitute termination for breach of the Agreement. DSOA shall have a right to terminate the Agreement if you unreasonably object to any such changes.

9. TERM

On termination or expiration of the Agreement, this DPA shall survive and continue in full effect until DSOA has returned, destroyed, and/or deleted all of Your Personal Data.

ANNEX 1 DATA PROCESSOR TERMS

1. GENERAL TERMS

- (a) The subject-matter, duration, nature, and purpose of the processing, the types Personal Data and the categories of individuals whose Personal Data is processed by DSOA under the DPA are described in Clause 2.2 of the DPA.
- (b) Each Party shall comply with its obligations under Data Protection Laws in relation to the processing of Your Personal Data. DSOA shall immediately inform you if it can no longer meet its obligations under the DPA or any Data Protection Law. You may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data by DSOA. Without limiting the foregoing, upon written notice from you, DSOA will immediately cease processing Your Personal Data if, in your reasonable opinion such processing is unauthorized or violates any Data Protection Law.
- (c) DSOA shall:
 - (i) only process Your Personal Data (including the transfer of Your Personal Data internationally) in accordance with your written instructions;
 - (ii) inform you if, in DSOA's opinion, your instructions would breach Data Protection Laws; and
 - (iii) assist you with assessments of the impact of processing Your Personal Data, and any consultations with a Data Protection Authority, as required under Data Protection Laws.
- (d) DSOA shall not:
 - (i) (A) sell or share (as such terms are defined by Data Protection Laws) Your Personal Data, or (B) retain, use, or otherwise disclose Your Personal Data for any purpose other than to provide, support, and improve the Services as specified in the Agreement or outside of the direct business relationship between DSOA and you; or
 - (ii) combine Your Personal Data with Personal Data DSOA receives from, or on behalf of, another person or persons, or which DSOA collects from its own interactions with an individual, except as permitted by applicable Data Protection Laws.

DSOA certifies that it understands the restrictions in Clause 1(d) of this Annex 1 and will comply with them.
- (e) Without limiting Clause 1(c)(i) of this Annex 1, DSOA shall promptly inform you if it is required to process Your Personal Data by any Applicable Law.

2. INDIVIDUAL RIGHTS

DSOA shall:

- (a) assist you, by appropriate technical and organisational measures, to fulfil and respond to any request by a Data Subject to exercise its rights under Data Protection Laws; and
- (b) if a Data Subject makes a written request to DSOA to exercise any of its rights under Data Protection Laws in relation to Your Personal Data, promptly forward you such request.

3. SECURITY MEASURES

- (a) DSOA shall implement and maintain appropriate technical and organisational security measures, including the measures set out in the Security Schedule; and
- (b) Without prejudice to the requirements of the Security Schedule, DSOA shall notify you promptly and without undue delay, and in any event within seventy-two (72) hours, after becoming aware of any Personal Data Breach relating to Your Personal Data. DSOA will provide you with a written report regarding the extent of data exposure, including the number and identity of affected individuals, if known, the status of remediation efforts and other relevant information, and keep you updated on any material developments, in each case, as required by Data Protection Laws. DSOA will institute appropriate controls to maintain and preserve all documents, records, and other data relating to any Personal Data Breach, in each case, as required by Data Protection Laws.

4. SUB-PROCESSORS; STAFF

DSOA shall:

- (a) **Appointment of Sub-Processors.** You acknowledge and agree that DSOA may engage Sub-processors in connection with the provision of Services. DSOA has or will enter into a written agreement with each Sub-processor containing appropriate data protection obligations with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- (b) **Notification of New Sub-Processors.** DSOA shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to process Personal Data in connection with the provision of the applicable Services.
- (c) **Objection Right for New Sub-Processors.** You may object to DSOA's use of a new Sub-processor where there are reasonable grounds to believe that the new Sub-processor will be unable to comply with the terms of this DPA, the Agreement, or Data Protection Laws. If you object to DSOA's use of a new Sub-processor, you must notify DSOA in writing within ten (10) days after notification regarding such new Sub-processor. Your failure to object in writing within such time period shall constitute approval to use the new Sub-processor. You acknowledge that the inability to use a particular new Sub-processor may result in delay in performing the Services, inability to perform the Services, and/or increased Fees for the Services. DSOA will notify you in writing of any change to Services and/or Fees that would result from DSOA's inability to use a new Sub-processor to which you have objected. You may either execute a written amendment to the Agreement implementing such change or exercise your right to terminate the Agreement in accordance with the termination provisions thereof. Such termination shall not constitute termination for breach of the Agreement. DSOA shall have a right to terminate the Agreement if you unreasonably object to a new Sub-Processor, or do not agree to a written amendment to the Agreement implementing changes in Services and/or Fees resulting from the inability to use the new Sub-processor at issue.
- (d) **Liability.** DSOA shall be liable for the acts and omissions of its Sub-processors to the same extent DSOA would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. COMMUNICATIONS

DSOA shall promptly notify you if it receives any communication (from a Data Subject, a Data Protection Authority or otherwise) which relates to the processing of Your Personal Data, or to either Party's compliance with Data Protection Laws, and shall assist you in responding to any such communication as required by Data Protection Laws.

6. COMPLIANCE AND AUDIT

Upon your reasonable written request, DSOA shall:

- (a) provide all information necessary to demonstrate compliance with the DPA; and
- (b) without limiting any of your other rights under the DPA or the Agreement, allow you or an auditor appointed by you to, at least once every twelve (12) months, to carry out an Audit. Without limiting Clause 6 of this Annex 1 or the requirements of the Security Schedule, DSOA shall retain a qualified and independent assessor to perform an annual audit of the physical, technical, administrative, and organizational safeguards put in place by DSOA that relate to the protection of the security, confidentiality, or integrity of Personal Data using an appropriate and industry accepted control standard or framework and assessment procedure. DSOA will provide the most current report of such assessment to you upon your request. You agree to: (i) review such report prior to requesting an Audit; (ii) ensure that all information obtained or generated by you or your auditor in connection with an Audit is kept strictly confidential (save for disclosure to a Data Protection Authority or as otherwise required by Applicable Law); (iii) ensure that the Audit or inspection is undertaken during normal business hours, with minimal disruption to DSOA's business, the Sub-processors' business, and the business of other customers of DSOA; and (iv) reimburse DSOA for reasonable costs undertaken by DSOA in assisting with the provision of information and allowing for and contributing to an Audit.

7. DATA PROTECTION IMPACT ASSESSMENT AND DATA PROTECTION AUTHORITY

Upon your request, DSOA shall provide you with reasonable cooperation and assistance needed to fulfil your obligation under Applicable Laws to carry out a data protection impact assessment related to your use of the Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to DSOA. Where required by Applicable Law, DSOA shall provide reasonable assistance to you in complying with a Data Protection Authority request or correspondence in the performance of your tasks relating to this DPA. You agree to reimburse DSOA for reasonable costs undertaken by DSOA in assisting you under this Clause 7.

8. TERMINATION AND EXPIRY

- (a) Unless expressly stated otherwise in the Agreement, upon termination or expiry of the Agreement, DSOA shall, and shall procure that each Sub-processor shall:
- (i) immediately cease to use Your Personal Data; and
 - (ii) at your option and in accordance with your instructions, return Your Personal Data to you, or delete Your Personal Data and all copies and extracts of Your Personal Data.
- (b) Without limiting Clause 8(a) of this Annex 1, DSOA shall inform you if it is required to retain a copy of any Your Personal Data after the termination or expiry of the Agreement by any Applicable Law.

ANNEX 2

Company Security Schedule

1. **Information Security Program.** Togetherwork Operations, LLC (“**Company**”), an affiliate of DSOA, maintains an information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing of Personal Data and the associated risks, are appropriate to (i) the types of Personal Data that DSOA will process; and (ii) the need for the security and confidentiality of such Personal Data. In formulating and implementing Company's information security program, Company has attempted to (i) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing Personal Data; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Data; (iii) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (iv) design and implement a plan that puts safeguards in place to reduce those risks; and (v) regularly monitor the effectiveness of those safeguards.
2. **Data Security Coordinator.** Company has designated an individual to supervise the implementation and maintenance of its information security program.
3. **Security Awareness and Training.** Company provides appropriate security awareness and training to its employees on relevant elements of Company's information security program.
4. **Physical Security.** Company uses, or contractually obligates its third-party vendors to use, safeguards that provide reasonable assurance that access to physical servers at the data centers storing Personal Data are limited to properly authorized individuals. Company also uses, or contractually obligates its third-party vendors to use, environmental controls to detect, prevent, and control environmental hazards. Controls include logging and monitoring of data center access, CCTV surveillance systems, and uninterruptable power supply modules and backup generators that provide backup power in the event of an electrical failure.
5. **Access Controls.** Company uses administrative and technical controls to: (i) limit access to its information systems and the facilities in which they are housed to authorized personnel; (ii) prevent personnel and others that should not have access to Personal Data from obtaining access; and (iii) remove access in the event of a change in job status.
6. **Security in Storage and Transmission.** Company uses technical controls to protect against unauthorized access to Personal Data that is transmitted over public electronic communications networks or stored in Company's systems, including encryption of sensitive data stored on laptops and removable storage devices.
7. **Retention and Disposal.** Company maintains policies and procedures regarding retention periods for Personal Data and for the secure disposal of devices containing Personal Data.
8. **Security Incident Procedures.** Company maintains incident response policies and procedures to be followed in the event of any security incident affecting Personal Data. Company's security incident procedures define roles and responsibilities for incident responses, including investigation, internal and external reporting, mitigation, and remediation.
9. **Contingency Planning.** Company maintains policies and procedures for responding to an emergency or other occurrence that could damage Personal Data. Company's procedures include periodically backing up production

systems and databases and maintaining formal disaster recovery and business continuity plans.

10. **Systems Monitoring.** Company monitors networks and systems to detect and log events that could cause problems.
11. **Change Management.** Company maintains policies and procedures for managing changes Company makes to its production systems, applications, and systems that process Personal Data.
12. **Third-Party Vendor Management.** Company evaluates the ability of each of its third-party service providers to protect the Personal Data to which Company has permitted them access and takes steps reasonably necessary to validate that such third-party service providers are applying appropriate security measures.
13. **Periodic Evaluation.** Company reviews the scope of its security measures periodically, including when there is a material change in Company business practices that may implicate the security or integrity of records containing Personal Data.