DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") forms part of the Terms of Use available at https://clickhelp.com/legal/terms-of-use/ ("Terms") or other written or electronic agreement ("Agreement") between:

(i) ClickHelp AM LLC, Davtashen, 3rd district, building 30, office 26, 0054 Yerevan, Armenia ("**Processor**"), and

(ii) the entity accepting the Terms or entering into such Agreement, acting on its own behalf and, where applicable, in the name and on behalf of its Affiliates ("**Controller**"),

each individually referred to as a "Party" and collectively as the "Parties".

This Addendum sets forth specific data processing terms and conditions governing the processing of Personal Data provided by Controller to Processor under the GDPR, UK GDPR, US Data Protection Laws, and other applicable data protection laws.

This Addendum becomes effective automatically on the date the Controller accepts the Terms or enters into such Agreement ("Effective Date").

References in this Addendum to the Terms or Agreement include those Terms or Agreement as amended or supplemented by this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

(a) "**Addendum Effective Date**" has the meaning given to it in section 2;

(b) "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Controller or Processor (as the context allows), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

(c) "**Controller Personal Data**" means any Personal Data that is (i) Processed by Processor on behalf of Controller, or (ii) otherwise Processed by Processor, in each case pursuant to or in connection with instructions given by Controller in writing, consistent with the Terms and (ii) subject to Data Protection Laws;

(d) **"Standard Contractual Clauses"** means the standard contractual clauses for the transfer of personal data to third countries pursuant to

GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, Module 2 (Controller-to-Processor), as amended or replaced from time to time;

(e) "**Data Protection Laws**" means (i) Directive 95/46/EC and, from 25 May 2018, Regulation (EU) 2016/679 ("GDPR") together with applicable legislation implementing or supplementing the same or otherwise relating to the processing of Personal Data of natural persons, (ii) to the extent not included in sub-clause (i), the Data Protection Act 1998 of the United Kingdom, as amended from time to time, and including any substantially similar legislation that replaces the DPA 1998, and (iii) the national legislation of the Swiss Confederation on the protection of Data Subjects with regard to the processing of Personal Data and on the free movement of such data, as amended from time to time, and other data protection or privacy legislation in force from time to time in the Swiss Confederation; and

(f) **"UK GDPR"** means the General Data Protection Regulation (EU) 2016/679 as applicable under UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018;

(g) **"UK Standard Contractual Clauses"** means the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the UK Information Commissioner on 2 February 2022;

(h) **"US Data Protection Laws"** means all applicable U.S. data privacy laws, including without limitation the California Consumer Privacy Act ("CCPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), the Utah Consumer Privacy Act ("UCPA"), and the Virginia Consumer Data Protection Act ("VACDPA"), as amended or replaced from time to time;

(i) "**Services**" means the services to be supplied by Processor to Controller pursuant to the Terms.

1.2 The terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**" and "**Processor**" have the same meanings as described in the Data Protection Laws and cognate terms shall be construed accordingly.

1.3 Capitalized terms not otherwise defined in this Addendum shall have the meanings ascribed to them in the Terms.

2. Formation of this Addendum

The Parties agree that this Addendum is deemed agreed by the Parties, and comes into effect, on the Addendum Effective Date, being the earlier of (i) the date that this Addendum is signed by Controller; and (ii) fifteen (15) calendar days after the date on which this Addendum is sent by Processor to Controller ("**Reception Date**"), except where Processor receives in writing Controller's objections to the terms of this Addendum within thirty calendar days of the Reception Date. The Parties shall then work together promptly and in good faith to resolve Controller's objections and to agree on a form of this Addendum acceptable to the Parties, in

which case the Addendum Effective Date shall be the date on which the agreed form of the Addendum is signed by the Parties.

3. Roles of the Parties

The Parties acknowledge and agree that with regard to the Processing of Controller Personal Data, as more fully described in **Annex 1** hereto, Controller acts as a Controller and Processor acts as a Processor.

The Parties expressly agree that Controller shall be solely responsible for ensuring timely communications to Controller's Affiliates who receive the Services, insofar as such communications may be required or useful in light of applicable Data Protection Laws to enable Controller to comply with such Laws.

4. Description of Personal Data Processing

In **Annex 1** to this Addendum, the Parties have mutually set out their understanding of the details of the Processing of the Controller Personal Data to the extent Processed by Processor pursuant to this Addendum, as required by Article 28(3) of the GDPR. Either Party may make reasonable amendments to **Annex 1** by written notice to the other Party and as reasonably necessary to meet those requirements. **Annex 1** does not create any obligation or rights for any Party.

5. Data Processing Terms

5.1. Processor shall:

5.1.1. Process the Controller Personal Data solely on the documented instructions of Controller, for the purposes of providing the Services and as otherwise necessary to perform its obligations under the Terms including with regard to transfers of Controller Personal Data to a third country outside the European Union or an international organization (unless required by Union or Member State law to which Processor is subject, in which case Processor shall inform Controller, if applicable, of that legal requirement before such Processing, unless that law prohibits such information on important grounds of public interest). Processor shall immediately inform Controller if, in Processor's opinion, an instruction infringes applicable Data Protection Laws;

5.1.2. ensure that persons authorized to Process the Controller Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

5.1.3. implement and maintain the technical and organizational measures set out in the Terms [**Annex 2** hereto], which the Parties have mutually agreed pursuant to Article 32 of the GDPR, having regard to the assessment of the appropriate level of security for Controller Personal Data and the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access or damage to such Personal Data;

5.1.4. be expressly and specifically authorized by Controller to engage another Processor to Process the Controller Personal Data ("Sub-Processor"), and specifically the Sub-Processors listed in Annex 3 hereto, subject to

Processor:

a. notifying Controller of any intended changes to its use of Sub-Processors listed in Annex 3 by emailing notice of the intended change to Controller at least 30 days in advance. Controller shall have 14 days from the date of such notice to object in writing to the use of the proposed Sub-Processor. If Controller objects, the Parties will, within the subsequent 14-day period, work together in good faith to find a commercially reasonable solution that avoids the use of the objected-to Sub-Processor.

   If no commercially reasonable solution is found within these 14 days, Controller shall have the right to terminate the affected Services by providing written notice within the remaining period until the new Sub-Processor is engaged. If Controller does not terminate the affected Services within this period, Processor may proceed to engage the new Sub-Processor;

b. including data protection obligations in its contract with each Sub-Processor which are materially the same as those set out in this Addendum; and

c. remaining liable to Controller for any failure by each Sub-Processor to fulfill its obligations in relation to the Processing of the Controller Personal Data;

5.1.5. to the extent legally permissible, promptly notify Controller of any communication from a Data Subject regarding the Processing of Controller Personal Data, or any other communication (including from a supervisory authority) relating to any obligation under the Data Protection Laws in respect of the Controller Personal Data and, taking into account the nature of the Processing, assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR;

5.1.6. Processor shall notify Controller without undue delay and in any event within 48 hours upon becoming aware of any Personal Data Breach affecting Controller Personal Data, providing sufficient details to enable Controller to meet its obligations under applicable Data Protection Laws;

5.1.7. assist Controller with its obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and information available to Processor;

5.1.8. upon termination or expiry of the Agreement, Processor shall, at the option of Controller, delete or return all Controller Personal Data and

delete existing copies, unless applicable law requires retention. Such deletion shall occur no later than within 90 days following termination or expiry, during which period the Processor shall maintain the security and confidentiality of the Controller Personal Data;

5.1.9. no more than once a year (unless requested by a supervisory authority), make available to Controller all information necessary to demonstrate compliance with the obligations laid down in GDPR Article 28 and allow for and contribute to audits, including inspections, conducted by Controller or an auditor mandated by. Controller shall bear the cost for audits or inspections, including, without limitation, reasonable Processor time, out of pocket expenses and consultancy fees.

5.1.10. Processor shall not directly or indirectly sell or share any Controller Personal Data, as defined by applicable US Data Protection Laws.

6. Transfers

Controller (as "data exporter") and Processor (as "data importer"), with effect from the commencement of the relevant transfer, hereby enter into the Controller to Processor SCCs (*mutatis mutandis*, as the case may be) in respect of any transfer (or onward transfer) from Controller to Processor where such transfer would otherwise be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address Data Protection Laws). Appendix 1 to the Controller to Processor SCCs shall be deemed to be prepopulated with the relevant sections of **Annex 1** to this Addendum and the processing operations are deemed to be those described in the Terms. Appendix 2 to the Controller to Processor SCCs shall be deemed to be prepopulated with **Annex 3** to this Addendum.

For transfers of personal data from the United Kingdom to countries without adequate protection, the Parties agree to incorporate the UK Standard Contractual Clauses in addition to the Standard Contractual Clauses (EU SCCs), with necessary modifications.

7. Indemnity

To the extent permissible by law, Processor shall indemnify and hold harmless Controller against all (i) losses, (ii) third party claims, (iii) administrative fines and (iv) costs and expenses (including, without limitation, reasonable legal, investigatory and consultancy fees and expenses) reasonably incurred in relation to (i), (ii) or (iii), suffered by Controller and that arise from any breach by Processor of this Addendum or of its obligations under applicable Data Protection Laws.

8. Severability

The Parties agree that, if any section or sub-section of this Addendum is held by any court or competent authority to be unlawful or unenforceable, it shall not invalidate or render unenforceable any other section of this Addendum.

9. Precedence

The provisions of this Addendum are supplemental to the provisions of the Terms. In the event of any inconsistency between the provisions of this Addendum and the provisions of the Terms, the provisions of this Addendum shall prevail.

IN WITNESS WHEREOF, this Data Processing Addendum ("Addendum") is entered into and becomes binding upon the Parties as of the date the Controller accepts the Terms of Use ("Effective Date").

Processor:
ClickHelp AM LLC, Davtashen, 3rd district, building 30, office 26, 0054 Yerevan, Armenia
Authorized Signatory: Aleksandr Muravev, Director

Controller:
The entity accepting the Terms of Use.

Annex 1: Description of Processing of Controller Personal Data

This Annex includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the Processing of the Controller Personal Data are set out in original Terms agreed upon by the parties.

The nature and purpose of the Processing of the Personal Data

The nature and purpose of the Processing of the Controller Personal Data are set out as described in original Terms agreed upon by the parties.

The categories of Data Subject to whom the Controller Personal Data relates

People registered in the documentation portal owned by the Controller and operated by the Processor.

The types of Controller Personal Data to be Processed

User ID, First Name, Last Name, Email address, IP address

The obligations and rights of Controller

The principal obligations and rights of Controller are set out in original Terms agreed upon by the parties and in this Addendum.

Data exporter (as applicable)

Controller, which engages Processor for the services specified in the Terms.

Data importer (as applicable)

Processor, which provides the services to Controller pursuant to the Terms.

Processing operations (as applicable)

The personal data transferred will be subject to the following basic processing activities:

- Service provision
- Customer support
- Customer relations management
- Sales and finance operations

AI Features Out of Scope. The parties acknowledge that AI features are intended solely for non-personal content and must not be used with personal data. Processing related to AI features is outside the scope of this DPA; third-party AI providers engaged for AI features are not sub-processors under this DPA.

Annex 2: Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood for the rights and freedoms of natural persons, Processor shall implement appropriate technical and organizational measures as set forth in the Terms.

These measures include, but are not limited to:

- Asset Classification and Control
  Processor's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that might be tracked include:
  - information assets, such as identified databases, disaster recovery plans, data classification, archived information;
  - software assets, such as identified applications and system software;
  - physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers, and communications equipment.

- Employee Screening, Training and Security
  - Screening/background checks: Where reasonably practicable and appropriate, as part of the employment/recruitment process, Processor performs employee screening and background checks on employees or prospective employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to the Processor's networks, systems, or facilities.
  - Identification: Processor requires all employees to provide proof of identification and any additional documentation that may be required based on the country of hire.
  - Training: Processor's annual compliance training program includes a requirement for employees to complete an online data protection and information security awareness.
  - Confidentiality: Processor ensures its employees are legally bound to protect and maintain the confidentiality of any data they handle pursuant to standard agreements.

- Communication and Information

- Processor performs logging of core information, including but not limited to development, financial transactions, payroll, and expenses.
- Processor has implemented policies and procedures for significant processes, which are made available to all personnel and/or contractors.
- Planned or emergency system changes are communicated internally to all relevant stakeholders.
- status.clickhelp.com is used by Processor to inform its customers and stakeholders of incidents and availability and major maintenance operations. Users can subscribe to email updates to this status page.

- Risk Assessment
  - The information security function is owned by the Operations Team and the CIO as its manager. The team meets regularly with the legal team and with top managers to review risk assessments and security policies.
  - Appropriate levels of Processor's management are involved in the risk management process, and risk identification considers both internal and external factors and their impact on the achievement of goals.
  - As a part of the risk management process, risk assessment includes management's decision on how internal and external risk should be managed (whether to accept, avoid, reduce or share the risk) and considers potential fraudulent activities.
  - Processor performs annual, periodic and ad-hoc information security assessments.

- Control Activities
  - Processor's products are always built and deployed from source code stored at source-code-management systems like Github.
  - Before deploying to production, any deployment is tested on non-production environments and tested by engineers and a dedicated QA team. No production infrastructure is used for testing.
  - All changes to the software are logged.

- Data Transmission Control and Encryption
  - Processor shall, to the extent it has control over any electronic transmission or transfer of personal data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. In particular, Processor shall:
    - implement industry-standard encryption practices in its transmission of personal data. Industry-standard encryption methods used by Processor includes Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);

        - for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on network that contains such information, a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

- System Access Controls
  Access to Processor's systems is restricted to authorized users. Formal procedures and controls govern how access is granted to authorized individuals and the level of access that is required and appropriate for that individual to perform their job duties.

- Data Access Control
  Processor applies the controls set out below regarding the access and use of personal data:
    - personnel are instructed to only use the minimum amount of personal data necessary in order to achieve relevant business purposes;
    - personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;
    - third party use of personal data is governed through contractual terms and conditions between the third party and Processor which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services.

- System Development and Maintenance
  Publicly released third party vulnerabilities are reviewed for applicability in the Processor environment. Based on risk to One Identity's business and customers, there are predetermined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Annex 3: List of Authorized Sub-Processors

Name	Scope	Company Location
Atlassian Pty Ltd	Project and Service Management Client Communication	Level 6, 341 George St, Sydney NSW 2000, Australia
Cobisi Research	Infrastructure and Services	Via Prima Strada 35 35129, Padova Italy (European Union)
Pipedrive OÜ	Customer relationship management (CRM), client communication, sales management, contact database management	Mustamäe tee 3a, 10615 Tallinn, Estonia (European Union)
Digital Realty Trust	Infrastructure and Services	5707 Southwest Parkway Building 1, Suite 275 Austin, TX 78735
European Data Hub	Infrastructure and Services	12D, Impasse Drosbach L-1882 Luxembourg
G-Core Labs S.A.	Infrastructure and Services	2-4, Rue Edmond Reuter L-5326 Contern, Luxembourg
Google, LLC	Client Communication Infrastructure and Services	1600 Amphitheatre Parkway, Mountain View, California, U.S.
Amazon Web Services, Inc.	Infrastructure and Services	410 Terry Ave. North, Seattle, WA 98109-5210
Microsoft Corporation	Infrastructure and Services	One Microsoft Way Redmond, Washington 98052 USA
PAYPRO GLOBAL, INC.	Payment Processing	225 The East Mall, Suite 1117, Toronto, Ontario, Canada, M9B 0A9
Typeform S.L.	Client Communication	CALLE BAC DE RODA (LO) 163 08018, BARCELONA Spain
Calendly, LLC	Client Communication	271 17th St NW, Ste 1000, Atlanta Georgia, 30363, United States
PostHog, Inc.	Product analytics, feature usage analytics, troubleshooting and customer support	2261 Market St #4008, San Francisco, CA 94114, United States