Last Updated: Oct 3, 2023

Data Processing Agreement

This Data Processing Agreement ("DPA") forms a part of the legal agreement ("Agreement"), as outlined in the Terms, entered into by and between Cloze, Inc. ("Cloze") and the user of the Cloze Platform ("Customer"), collectively the "Parties." The purpose of the DPA is to ensure such processing is conducted in accordance with applicable Data Protection Laws (defined below).

This DPA is supplemental to the Agreement and sets out the terms that apply when: (i) Personal Data (defined below) is processed by Customer, who acts as Data Controller, under the Agreement; (ii) Cloze acts as Data Processor of Customer Account Data; (iii) The Customer wishes to contract the Services as set forth in the Terms, which imply the processing of Personal Data by the Data Processor. Further details of the Processing are set out in Exhibit A to this DPA.

Customer acknowledges that by agreeing to the Terms, they are also agreeing to this DPA. To the extent that there are any conflicting provisions between the Terms and this DPA with regard to the processing of Personal Data, this DPA shall prevail. The effective date of this DPA is the same date that the Customer agreed to the Terms.

1. Definitions. All capitalized terms not defined in Section 1 of this DPA or otherwise defined in other sections of this DPA, shall have the meanings set forth in the Agreement, GDPR, Cloze Privacy Policy, or Terms, as applicable.

1.1 "Sub-Processor" means any person appointed by or on behalf of Data Processor to process Customer Personal Data on behalf of the Customer in connection with the DPA.

1.2 "Customer Account Data" means all data (including Personal Data) that relates to Customer's relationship with Cloze. Customer Account Data includes any data Cloze may need to collect for the purpose of managing its relationship with Customer, or as otherwise required by applicable laws and regulations.

1.3 "Data Exporter" means Customer.

1.4 "Data Importer" means Cloze.

1.5 "Data Protection Laws" means all data protection legislation and regulations applicable to the processing of the Customer's Personal Data under this DPA and the Terms, including supplementing national legislation, in each case as updated, amended, repealed, consolidated, or replaced from time to time. The terms "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth under applicable Data Protection Laws.

1.6 "Data Subject" means an individual that is protected under any applicable Data Protection Law.

1.7 "DPA" means this Data Processing Agreement and all Exhibits.

1.8 "EU SCCs" or "Standard Contractual Clauses" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of Personal Data to countries not otherwise recognized as offering an adequate level of protection for Personal Data by the European Commission (as amended and updated from time to time).

1.9 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Controller to the Data Processor (or its premises) outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.10 "ex-UK Transfer" means the transfer of Personal Data, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Controller to the Data Processor (or its premises) outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.11 "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and all supplementing legislation, in each case as may be amended, repealed, consolidated, or replaced from time to time.

1.12 "Personal Data" or any such variation of the term (such as "Personal Information" or "Personally Identifiable Information") shall have the meaning set forth under applicable Data Protection Laws.

1.13 "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Account Data, stored or otherwise processed by Cloze.

1.14 "Terms" mean the terms of service entered into between Cloze and Customer, which are available here.

2. Processing of Data Customer Account Data

2.1 Cloze, shall not process Personal Data (i) for purposes other than those set forth in the Agreement, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Customer, or (iii) in violation of Data Protection Laws. Customer hereby instructs Cloze to process Personal Data in accordance with the foregoing and as part of any processing initiated by Customer in its use of the Services.

2.2 Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer's instructions will not cause Cloze to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Cloze by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Cloze regarding the processing of such Personal Data. Customer shall not provide or make available to Cloze any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services and shall indemnify Cloze from all claims and losses in connection therewith.

2.3 The Parties agree that the details of the data processing subject to this DPA are outlined in Exhibit A.

2.4 CCPA. The Parties acknowledge that their relationship under the CCPA is governed by the CCPA Addendum to this DPA, listed in Exhibit D.

3. Deletion or Return of Customer Account Data

3.1 Following completion of the Services, at Customer's choice, Cloze shall securely delete Customer Account Data, unless further storage of such Customer Account Data is required or authorized by applicable Data Protection Laws. If return or destruction is impracticable or prohibited by law, rule, or regulation, Cloze shall take measures to block such Customer Account Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule, or regulation) and shall continue to appropriately preserve the confidentiality of the Customer Account Data remaining in its possession, custody, or control. By agreeing to this DPA, Customer authorizes Cloze, in accordance with this agreement to delete information when not reasonably needed for our Services.

4. Data Processor Personnel and Confidentiality.

4.1 Cloze shall take commercially reasonable steps to ensure that: (i) persons employed by Cloze; and (ii) other persons engaged at Cloze's place of business who may have access to the Customer Account Data (including Content), are aware of and comply with the terms set forth in this DPA, ensuring in each case that access is limited to those individuals who need to know or access the relevant Customer Account Data, as necessary for the purposes of the Terms.

5. Security of Customer Account Data; Security Incidents.

5.1 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 and severity for the rights and freedoms of natural persons, Cloze shall maintain reasonable technical and organizational security measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit C sets forth additional information about Cloze's technical and organizational security measures.

5.2 Cloze shall notify Customer without undue delay upon becoming aware of a Security Incident affecting Customer Account Data and will provide Customer with sufficient information to allow the Customer to meet any obligations to notify, report, or inform Data Subjects and Supervisory Authorities of the Security Incident under the Data Protection Laws.

5.3 Cloze shall cooperate with the Customer and take reasonably commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each such Security Incident. The obligations described in 5.1 and 5.2 do not apply to Security Incidents experienced by Customer, nor does compliance with such obligation's acknowledge liability on the part of Cloze.

6. Sub-Processing of Customer Account Data.

6.1 Customer acknowledges and agrees that Cloze may (1) engage or delegate Sub-Processors on the List (defined below) to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. For purposes of this Section, Customer consents to Cloze engaging Sub-Processors reasonably required to assist Cloze for the purposes of providing the Services.

6.2 Cloze maintains and provides Customer with a list of Sub-Processors (the "List") which can be found online here: https://www.cloze.com/app/legal/subprocessors. Cloze will inform the Data Controller, of changes in Sub-Processors in accordance with the procedure for modifying the Terms as described in Section 14. Customer may object to the modification of Sub-Processors used by Cloze by contacting Cloze at privacy@cloze.com. However, Customer acknowledges that certain Sub-Processors are essential to providing the Services and that objecting to the use of a Sub-Processor may prevent Cloze from offering the Services to Customer.

6.3 When Cloze does engage Sub-Processors, it will enter into a written agreement with such Sub-Processor imposing on the Sub-Processor data protection obligations comparable to those imposed on Cloze under this DPA, with respect to the protection of Customer Account Data. In case a Sub-Processor fails to fulfill its data protection obligations under such written agreement with Cloze, Cloze will remain liable to Customer for the performance of the Sub-Processor's obligations under such agreement.

6.4 If Customer and Cloze have entered into Standard Contractual Clauses as described in Section 7 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Cloze of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the Parties agree that the copies of the agreements with Sub-Processors that must be provided by Cloze to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information or the UK IDTA or UK Addendum (as applicable), or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Cloze beforehand, and that such copies will be provided by Cloze only upon request by Customer.

7. Transfers of Personal Data

7.1 The Parties agree that Cloze may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Cloze's primary processing operations take place in the United States, and that the transfer of Customer Account Data to the United States is necessary for the provision of the Services to Customer. If Cloze transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Cloze will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

7.2 Ex-EEA Transfers. The Parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

7.2.1 Module Two (Controller to Processor) of the EU SCCs applies when Customer is a controller and Cloze is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.

7.2.2 Module Three (Processor to Sub-Processor) of the EU SCCs applies when Customer is a processor and Cloze is processing Personal Data on behalf of Customer as a Sub-Processor.

7.3 For each module, where applicable the following applies:

7.3.1 The optional docking clause in Clause 7 does not apply.

7.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Sub-Processor changes shall be as set forth in Section 6.2 of this DPA;

7.3.3 In Clause 11, the optional language does not apply;

7.3.4 All square brackets in Clause 13 are hereby removed;

7.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by Irish law;

7.3.6 In Clause 18(b), disputes will be resolved before the courts of Ireland;

7.3.7 Exhibit B to this DPA contains the information required in Annex I of the EU SCCs;

7.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and

7.3.9 By entering into this DPA, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

7.4 Ex-UK Transfers. The Parties agree that ex-UK Transfers are made pursuant to the provisions set forth in this section, whichever applies.

7.4.1 Data Exports from the United Kingdom under the International Data Transfer Agreement. For ex-UK Transfers, the Mandatory Clauses of the Approved IDTA ("Mandatory Clauses"), being the template IDTA A.1.0 issued by the UK Information Commissioner's Office ("ICO") and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses shall apply.

(i) The information required for Table 1 of Part One of the IDTA is set out in Exhibit B of this DPA and below.

a. The start date of the IDTA is the effective date of this DPA.

b. The Data Exporter's full legal name, trading name, official registration number, address, and key contact person details will be as entered in relation to the Agreement.

c. By entering into the Agreement, the Parties agree to be bound by the IDTA, as applicable.

(ii) The information required for Table 2 of Part One of the IDTA is set out in Exhibits A and B of this DPA and below.

a. The Data Importer (processor or sub-processor) and Data Exporter (controller or processor) are known as the "Parties."

b. The law of England and Wales governs the IDTA.

c. England and Wales are the primary place for legal claims to be made by the Parties.

d. The UK GDPR applies to the Data Importer's processing of the transferred data.

e. The Data Importer may process the transferred data for the period for which the DPA is in force.

f. The Parties can end the IDTA before the end of the term of the IDTA by serving three months' written notice in accordance with the Mandatory Clauses set forth in Part 4 of the IDTA.

g. The Data Importer may end the IDTA when the IDTA changes, in accordance with the Mandatory Clauses set forth in Part 4 of the IDTA.

h. The Data Importer may transfer on the transferred data to another organisation or person (who is a different legal entity) under the Mandatory Clauses set forth in Part 4 of the IDTA. There are no specific restrictions on when the Data Importer may forward the transferred data.

i. The Parties must review the security requirements (as set forth in Section 7.4.1(iv) below) each time there is a change to the transferred data, purposes, Data Importer information, transfer risk assessment (TRA), or risk assessment.

(iii) The information required for Table 3 of Part One of the IDTA is set out in Exhibits A and B of this DPA and below.

a. The categories of transferred data, categories of special categories, and criminal records data, and the categories of Data Subjects will update automatically if the information is updated in the DPA.

b. The Data Importer may process the transferred data for the purposes set out in Exhibits A and B of this DPA. The purposes will update automatically if the information is updated in the DPA.

(iv) The information required for Table 4 of Part One of the IDTA is set out in Exhibit C of this DPA. The security requirements will update automatically if the information is updated in

the DPA.

7.4.2 Data Exports from the United Kingdom under the Standard Contractual Clauses. For ex-UK Transfers where the EU SCCs also apply, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the UK ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply. The information required for Tables 1 and 3 of Part One of the Approved Addendum is set out in Exhibits B and C of this DPA, as well as below. The information required for Table 2 of Part One of the Approved Addendum is set out in Section 7.2 of this DPA. For the purposes of Table 4 of Part One of the Approved Addendum, the Data Importer may end the Approved Addendum when it changes.

(i) The start date of the Approved Addendum is the effective date of this DPA.

(ii) By entering into the Agreement, the Parties agree to be bound by the Approved Addendum, as applicable.

7.5 Transfers from Switzerland. The Parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

7.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

7.5.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

7.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

7.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

7.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

7.6.1 As of the date of this DPA, Cloze has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer Account Data ("Government Agency Requests");

7.6.2 If, after the date of this DPA, Cloze receives any Government Agency Requests, Cloze shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Cloze may provide Customer's basic contact information to the government agency. If compelled to disclose Customer Account Data to a law enforcement or government agency, Cloze shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Cloze is legally prohibited from doing so. Cloze shall not voluntarily disclose Customer Account Data to any law enforcement or government agency. The Parties shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such Government Agency Requests; and

7.6.3 The Parties will meet as needed to consider whether:

(i) the protection afforded by the laws of the country of Cloze (Data Importer) to Data Subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant

with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the Data Importer, taking into account all relevant information available to the Parties, together with guidance provided by the supervisory authorities.

8. Data Subject Rights.

8.1 Taking into account the nature of the Processing, Cloze shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

8.2 Cloze has provided Customer's with the tools necessary to correct, amend, or delete inaccurate data, and Customers may use these tools to comply with Data Subject requests related to the right to correct, amend, or delete inaccurate data.

8.3 Cloze shall:

8.3.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect to Customer Account Data.

8.3.2 advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Cloze, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

8.3.3 ensure that it does not respond to that request except on the documented instructions of Customer or as required by applicable laws to which Customer is subject, in which case Cloze shall to the extent permitted by applicable laws inform Customer of that legal requirement before Cloze responds to the request.

9. Actions and Access Requests; Audits.

9.1 Cloze shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA.

9.2 Upon Customer's written request at reasonable intervals (no more than every 12 months), and subject to reasonable confidentiality controls, Cloze shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Cloze's compliance with prevailing data security standards applicable to the processing of Customer's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Customer's independent third party representative to conduct an audit or inspection of Cloze's data security infrastructure and procedures that is sufficient to demonstrate Cloze's compliance with its obligations under Data Protection Laws, provided that (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Cloze's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Cloze for any time expended for on-site audits. The scope of such an audit will be agreed in advance and shall not involve physical access to the servers on which Customer Content and Personal Data is hosted.

9.3 Cloze shall, taking into account the nature of the processing and the information available to Cloze, provide Customer with reasonable cooperation and assistance where necessary for Customer to:

9.3.1 Comply with its obligations under Data Protection Laws to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Customer does not otherwise have access to the relevant information.

9.3.2 Cooperate and/or consult with any supervisory authority where necessary and where required by Data Protection Laws.

9.3.3 Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance provided by Cloze as described in 9.3.1 and 9.3.2.

Last Updated: Oct 3, 2023

Exhibit A

Details of Processing

Nature and Purpose of Processing: Cloze will process Customer Account Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA.

Duration of Processing: Cloze will process Customer Account Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Cloze's legitimate business needs; or (iii) by applicable law or regulation. Customer Account Data will be processed and stored as set forth in Cloze's Privacy Policy.

Categories of Data Subjects: Customer may submit Personal Data to Cloze for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Users of Customer's services.
- Employees and contractors of Customer.
- Any other Data Subjects whose information is provided to Cloze in the course of providing the Services to Customer.

Categories of Personal Data: Customer may submit Customer Account Data, which includes Personal Data, to Cloze for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Name
- Address
- E-mail address
- Log-In credentials, such as username, third party platform login credentials, or other Cloze login credentials
- Billing or payment information, including credit card numbers
- Contact records
- Communication records, including but not limited to e-mails, calendar entries, phone call logs, text messages, and social media messages
- Commercial information including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Professional or employment-related information
- Business information related to the day-to-day such as, notes, files, and other online documents, task lists, project, and deal records
- Internet or other electronic network activity information, such as Customer's cookies or other unique identifiers, log data, or web beacons
- Geolocation data, in order to enable synchronization of data between our Services
- Inferences drawn from any of the information identified above

Sensitive Data or Special Categories of Data: Customer is prohibited from processing any "Special Categories of Data" through the Services, as defined in the GDPR or the UK GDPR. Customer Content may contain "sensitive" Personal Data (as defined under other applicable Data Protection Laws), provided by Customer for the provision of the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include:

- Contents of Customer emails
- Text messages
- App messages

Last Updated: Oct 3, 2023

Exhibit B

The following includes, among other things, the information required by Annex I and Annex III of the EU SCCs, as well as the UK IDTA and UK Addendum (collectively, for purposes of Exhibit B, the "Clauses").

1. **The Parties**

Data Exporter(s): [*Identity and contact details of the data controller(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Full legal name: [_____]

Trading name (if different): [_____]

Official registration number (if any) (company number or similar identifier): [_____]

Address: [_____]

Key contact's name, job title, and contact details (including email): [_____]

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date: mm/dd/yyyy

Role (controller/processor): Controller

Data Importer(s): [*Identity and contact details of the data processor(s), including any contact person with responsibility for data protection]*

Full legal name: Cloze, Inc.

Address: 396 Washington St., Suite 138, Wellesley, Massachusetts 02481

Key contact's name, job title, and contact details (including email): privacy@cloze.com

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date: 2023-10-03

Role (controller/processor): Processor

2. **Description of the Transfer**

Data Subjects	The Data Exporter may submit Personal Data to the Data Importer through its software, services, systems, products, and/or technologies, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Laws and regulations, and which may include but is not limited to Personal Data relating to the following categories of Data Subjects: • Users of Customer's services. • Employees and contractors of Customer. • Any other Data Subjects whose information is provided to Cloze in the course of providing the Services to Customer.
Categories of Personal Data	The Personal Data transferred concern the following categories of data: • Name • Address • E-mail address

	• Log-In Credentials, such as username, Third Party Platform Login Credentials, or other Cloze Login Credentials • Billing or payment information, including credit card numbers • Contact records • Communication records, including but not limited to e-mails, calendar entries, phone call logs, text messages, and social media messages • Commercial information including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies • Professional or employment-related information • Business information related to the day-to-day such as, notes, files, and other online documents, task lists, project, and deal records • Internet or other electronic network activity information, such as Customer's cookies or other unique identifiers, log data, or web beacons • Geolocation data, in order to enable synchronization of data between our Services • Inferences drawn from any of the information identified above
Special Category Personal Data (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved	N/A
Nature of the Processing	Data is processed in order: to provide the Services as described in the Terms and in accordance with the Terms, including in this DPA, the Privacy Policy, and these Clauses.
Purposes of Processing	To fulfill each party's obligations under the Agreement.
Duration of Processing and Retention (or the criteria to determine such period)	During the term of the Agreement
Frequency of the transfer	During the term of the Agreement on a periodic basis throughout the day and/or at the discretion of Customer.
Recipients of Personal Data Transferred to the Data Importer	Cloze provided Customer with a link to the List which outlines Cloze's Sub-Processors in the DPA. Cloze's relationship with Sub-Processors is described in Section 6 of the DPA, as well as in the Terms.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13.

Last Updated: Oct 3, 2023

Exhibit C

Description of the Technical and Organizational Security Measures implemented by the Data Importer

"Technical and organizational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Cloze will maintain appropriate physical, administrative, technical, and organizational measures and safeguards for protection of the security, confidentiality, and integrity of the Data Exporter's Personal Data. More information on Cloze's technical and organizational measures can be found in the Privacy Policy and the Data Processing Agreement. Cloze will not materially decrease the overall security of the Services.

The following includes the information required by Annex II of the EU SCCs, as well as the UK IDTA and UK Addendum.

Technical and Organizational Security Measure	**Details**
Measures of pseudonymization and encryption of Personal Data	Cloze will ensure that aggregated information will not identify Customer personally.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Cloze will take appropriate steps to ensure its employees, authorized agents, and any Sub-Processors comply with and acknowledge and respect the confidentiality of content and Personal Data, including after the end of their employment, contract, or at the end of their assignment.
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	Cloze has Business Continuity and Data Recovery Policies, maintains multiple redundant application servers, replicated databases with automatic failover, hourly backups with off-site backup storage and customer initiated "on-demand" exports at any time.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Cloze maintains 24/7 event and vulnerability monitoring, uses anti-virus/malware protection, intrusion detection systems, runs a bug bounty program, and conducts 3rd party annual penetration testing and assessment.
Measures for user identification and authorization	Prior to complying with Customer requests, Cloze will first verify the identity of the customer by comparing the information provide by the individual making the request with the information Cloze has on file for the implicated customer. Customer's may authorize an agent to make requests on Customer's behalf. To designate an agent, Customer must provide a written and signed document by both the Customer and the agent that authorizes the agent to act on Customer's behalf. Customer may also use a power of attorney. Cloze will still require that Customer provide information to allow Cloze to reasonably verify that Customer is the person about whom Cloze collected Personal Data.
Measures for the protection of data during transmission	Cloze uses browser encryption using the current TLS version for communication with customers as well as internal transparent network-

	layer encryption of all traffic.
Measures for the protection of data during storage	Cloze uses encrypted storage, 3-way replicated databases with automatic failover and maintains multi-location backups.
Measures for ensuring physical security of locations at which Personal Data are processed	Data is secured at secure data centers provided by Amazon Web Services.
Measures for ensuring events logging	Cloze maintains automated logging and event monitoring using system level monitoring tools such as CloudWatch and multiple application level monitoring tools.
Measures for ensuring system configuration, including default configuration	Cloze regularly has independent auditing and penetration testing conducted, maintains secure and tested AWS AMI images, and builds new images from scripted bare metal installations.
Measures for internal IT and IT security governance and management	Cloze provides security awareness training and has Information Security and Mobile Device Policies that include acceptable use, password, and two-factor authentication policies.
Measures for certification/ assurance of processes and products	Cloze performs annual risk assessments and penetration testing, code reviews, and maintains a Secure Coding policy.
Measures for ensuring data minimization	Cloze does not collect information that is not necessary for the purposes outlined in Exhibit B of this DPA.
Measures for ensuring data quality	Cloze uses transactional databases, maintains 3 copies of all user data, and uses quorum consensus to ensure data is accurate.
Measures for ensuring limited data retention	Cloze retains Personal Data about Customer that is necessary to fulfill the purpose for which that information was collected or as required or permitted by law. We do not retain Personal Data longer than is necessary for Cloze to achieve the purposes for which we collected it. When we destroy Customer Account Data, Cloze do so in a way that prevents that information from being restored or reconstructed.
Measures for ensuring accountability	Cloze user permissions are assigned on a “least privilege” basis and all activity (login, access, add/update/delete, import, export) are logged in detailed audit trails by Cloze.
Measures for allowing data portability and ensuring erasure	To exercise the right of data portability Customer’s (or agents) may contact support@cloze.com. We will respond to request as soon as reasonably possible and within the timeframe required under applicable law.
Technical and organizational measures of Sub-Processors	The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Sub-Processor which imposes the same obligations on the Sub-Processor as are imposed on the Data Importer. Where the Sub-Processor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance

	of the Sub-Processor's obligations under such agreement. The prior written contract between the Data Importer and the Sub-Processor shall also provide for a third-party beneficiary clause for cases where the data subject is not able to bring the claim for compensation against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Sub-Processor shall be limited to its own processing operations under the Clauses. The provisions relating to data protection aspects for Sub-Processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established. The Data Exporter shall keep a List of Sub-Processing agreements concluded under the Clauses and notified by the Data Importer, which shall be updated at least once a year. The List shall be available to the Data Exporter's data protection supervisory authority.

Last Updated: Oct 3, 2023

Exhibit D

CCPA Addendum

This California Consumer Privacy Act Addendum ("CCPA Addendum") is incorporated as part of the DPA and sets out the terms that apply when Personal Data subject to the CCPA is processed by Cloze under the DPA. The purpose of the CCPA Addendum is to ensure such processing is conducted in accordance with the California Consumer Privacy Act and the California Privacy Rights Act.

1. **Definitions.** Any capitalized terms in this Addendum that is not otherwise defined in the DPA shall have the meaning given to that term in the CCPA.

2. **Representations and Warranties**

   2.1. Cloze represents and warrants that it is a Service Provider or Contractor for the purposes of the services it provides to Customer pursuant to the DPA and the Agreement.

3. **Cloze Processing of Customer Account Data (including Personal Data)**

   3.1. Cloze shall process Personal Data it receives pursuant to the Agreement only for the limited and specified purposes of providing the agreed upon services to Customer (as outlined in Exhibit A) and is prohibited from using Personal Data for any other purpose.

   3.2. Cloze shall comply with all applicable sections of the CCPA, including by providing the same level of protection to Personal Data as required by Customer under the law.

   3.3. Cloze agrees that Customer has the right to take reasonable and appropriate steps to ensure that Cloze uses Personal Data that it receives from or processes on behalf of Customer in a manner consistent with Customer's obligations under the CCPA.

   3.4. Cloze agrees that Customer has the right to take reasonable and appropriate steps to stop and remediate Cloze's unauthorized use of Personal Data.

   3.5. Cloze shall notify Customer as soon as possible after Cloze determines that it can no longer meet its obligations under the CCPA.

   3.6. If Cloze engages Sub-Processors in relation to providing services to Customer pursuant to the Agreement, Cloze shall have a contract with the Sub-Processor that complies with the CCPA and has the same restrictions on the processing of Personal Data as outlined in this Addendum.

4. **Restrictions on Cloze's Use of Personal Data**

   4.1. Cloze shall not Sell or Share Personal Data it receives from or processes on behalf of Customer, for purposes outside of those outlined in the DPA and exhibits incorporated by reference in the DPA.

   4.2. Cloze shall not retain, use, or disclose Personal Data it receives from or processes on behalf of Customer for any purpose (including any Commercial Purpose) other than for the purposes specified in the Agreement, DPA, and except as otherwise permitted by the CCPA.

   4.3. Cloze shall not retain, use, or disclose Personal Data it receives from or processes on behalf of Customer outside of the direct business relationship between Cloze and Customer, except as otherwise permitted under the CCPA.

   4.4. Cloze shall not combine the Personal Data it receives from or processes on behalf of Customer with Personal Data it receives from or on behalf of another person or which it collects from its own interaction with another individual, provided that Cloze may combine Personal Data to perform any Business Purpose, such as to analyze how users interact with Services, or as otherwise permitted under the CCPA.

5. **Consumer Requests**

5.1. Customer agrees to: (i) inform Cloze of any consumer request made pursuant to the CCPA that they must assist Customer to comply with and (ii) provide the information necessary for Cloze to comply with the request.