NINJIO, LLC
Data Protection Addendum

This Data Protection Addendum (this "DPA") is entered into by and between Ninjio, LLC ("Ninjio" or "Processor") and the counterparty (the "Company" or "Controller") to that certain agreement which incorporates this DPA by reference (the "Agreement") effective as of the effective date of the Agreement. Each of Processor and Controller may be referred to herein as a "Party" and collectively as the "Parties."

Recitals

WHEREAS, pursuant to the Agreement, Processor shall provide Controller with certain software, content, and/or services, as more specifically set forth in the Agreement;

WHEREAS, in connection with Processor's performance of the Agreement, the Parties anticipate that Processor may process certain Personal Data, including outside of the EEA and/or United Kingdom, as a Data Processor and/or Sub-processor, as more fully described herein; and

WHEREAS, this DPA sets forth the mandatory clauses required by Applicable Data Protection Laws and other undertakings in order to ensure that adequate safeguards are established with respect to the protection of such Personal Data in accordance with Applicable Data Protection Laws.

NOW, THEREFORE, the Parties, intending to be legally bound, hereby agree to the following terms, conditions, and undertakings:

Agreement

Section 1. Definitions. Capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement. The following terms shall have the following meanings:

"Adequate Jurisdiction" means a country, territory, specified sector, or international organization that is covered by a valid adequacy decision or adequacy regulation under Article 45 of the GDPR or the corresponding provisions of UK Data Protection Law, in each case only for so long as and to the extent such decision or regulation remains in effect.

"Affiliate" means, with respect to a Party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such Party (but only for so long as such Control exists). As used in this definition, the terms "control," "controlling" and "controlled by" shall mean the possession, directly or indirectly, of the power either to (a) vote 50% or more of the securities or interests having ordinary voting power for the election of directors (or other comparable controlling body) of such person or (b) direct or cause the direction of the actions, management or policies of such person, whether through the ownership of voting securities or interests, by contract or otherwise.

"Applicable Data Protection Laws" means all privacy, data protection, data security, breach-notification, and electronic-communications laws and binding regulations applicable to a Party's Processing under the Agreement, in each case as amended, replaced, or superseded from time to time. These include, where applicable, the GDPR; UK Data Protection Law; the CCPA; and other comprehensive U.S. state privacy laws, including the Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, Virginia Consumer Data Protection Act, and successor or substantially similar state laws.

"CCPA" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act.

"Complaint" means a complaint or request relating to either Party's obligations under the Applicable Data Protection Laws relevant to this DPA, including any compensation claim from a Data Subject or any notice, investigation, or other action from a Supervisory Authority.

"Data Subject" has the meaning given to Data Subject, Consumer, or any other analogous term under Applicable Data Protection Laws.

"Data Subject Request" means a request made by a Data Subject to exercise any rights of data subjects under Applicable Data Protection Laws.

"EEA" means the European Economic Area (i.e., the 27 member states of the European Union, together with Iceland, Liechtenstein, and Norway).

"EEA Standard Contractual Clauses" means the Standard Contractual Clauses set out in the Annex to the European Commission's Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, a completed copy of which comprises Appendix 2.

"GDPR" means the General Data Protection Regulation (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).

"Personal Data" means data that is Personal Data, Personal Information, or any other analogous term under Applicable Data Protection Laws that is Processed in connection with the Agreement.

"Process" shall have the same meaning under Applicable Data Protection Laws, and shall include, but is not limited to, any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, including access, adapt, alter, block, catalog, collect, combine, compile, consult, copy, cross-reference, erase, destroy, disclose, display, disseminate, download, input, log, make available, maintain, manage, organize, output, perform, provide, post, process, receive, retain, retrieve, record, reproduce, store, translate, submit, transmit, transfer, upload, use, or otherwise make other derivative works or improvements. "Processed" has a correlative meaning.

"Purpose" means the specific purposes set forth in the Agreement and as further set forth in Appendix 1 of this DPA.

"Public Authority" means any national, provincial, territorial, state, county, municipal, quasi-governmental or self-regulatory department, authority, law enforcement agency, national security agency, regulator, organization, agency, commission, board, tribunal, dispute settlement panel or body, bureau, official, minister, or court or other law, rule or regulation-making entity having or purporting to have jurisdiction over Controller Processor, or any Processing or other matter related to this DPA, including any Supervisory Authority

"Restricted Transfer" means a transfer of Personal Data (including an onward transfer) that requires an adequacy decision, appropriate safeguard, or derogation under Chapter V of the GDPR, UK Data Protection Law, or other Applicable Data Protection Laws. A transfer to an Adequate Jurisdiction, within the scope of the applicable adequacy decision or regulation, is not a Restricted Transfer.

"Sale" or "Sell" shall have the same meaning under Applicable Data Protection Laws.

"Share," "Shared," or "Sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data by a Party to another party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioural advertising for the benefit of a business in which no money is exchanged. For the avoidance of doubt, "Share" will also have the same definition as under the CCPA.

"Security Incident" means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Processor or a Sub-processor under the Agreement. Security Incident does not include unsuccessful attempts or activities that do not compromise Personal Data, such as pings, port scans, unsuccessful login attempts, denial-of-service attempts, or other attacks on firewalls or networked systems.

"Sensitive Personal Data," "Sensitive Data" or "Sensitive Information" shall have the same meaning under Applicable Data Protection Laws, and in any event shall include without limitation, the categories of sensitive Personal Data in Appendix 1. Notwithstanding anything to the contrary, Sensitive Personal Data, Sensitive Data and Sensitive Information will be included in references to Personal Data throughout this DPA.

"Services" means collectively, the software, content, and services provided by Processor under the Agreement.

"Standard Contractual Clauses" or "SCCs" means the EEA Standard Contractual Clauses and, for UK Restricted Transfers, the EEA Standard Contractual Clauses as modified by the UK Addendum.

"Sub-processor" means any third party, including an Affiliate of Processor, engaged by or on behalf of Processor to Process Personal Data on behalf of Controller in connection with the Services.

"Supervisory Authority" means an independent public authority established under Article 51 of the GDPR, the UK Information Commissioner, or any other regulator with authority over the relevant Processing.

"Third Party Data Source" means an entity other than Controller or Processor that may provide Personal Data in connection with the Services.

"Transfer Mechanism" means a legally valid mechanism for a Restricted Transfer, including an applicable adequacy decision or regulation, the SCCs, the UK Addendum, the EU-U.S. Data Privacy Framework or UK Extension where the recipient is validly certified and the transfer is within scope, or another appropriate safeguard approved under Applicable Data Protection Laws.

"UK Data Protection Law" means all laws relating to data protection, privacy, and electronic communications in force from time to time in the United Kingdom, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and each as amended by the Data (Use and Access) Act 2025.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, template B.1.0 issued by the UK Information Commissioner and laid before Parliament on 2 February 2022, as revised in accordance with its mandatory clauses, a completed copy of which comprises Appendix 3.

Section 2. Relationship between the Parties, DPA and the Agreement.

2.1. The Parties agree that this DPA will replace any existing data protection addendum or similar agreement the Parties may have previously entered into in connection with the Services.

2.2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of any conflict between this DPA and the Agreement, the conflicting provision of this DPA will prevail.

2.3. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of Data Subjects, are as described in Appendix 1.

2.4. Each Party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its Sub-processors comply), with all Applicable Data Protection Laws.

2.5. In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that Processor may act as a Data Processor (where

Company is a Data Controller) and/or a sub-processor (where Company acts as the Data Processor to its end user business clients that are the Data Controller), as described further in Annex 1.

Section 3. Processing of Personal Data by Processor.

3.1. With respect to all Personal Data, Processor warrants that it shall (and shall ensure each person acting under its authority shall):

(a) Process Personal Data only to provide the Services and for the Purpose, and only on Controller's documented instructions set out in the Agreement, this DPA, applicable order forms, and Controller's authorized use and configuration of the Services, including with respect to transfers of Personal Data, unless Processing is required by Applicable Data Protection Laws. If legally permitted, Processor shall inform Controller of that legal requirement before the Processing;

(b) promptly inform Controller if, in Processor's opinion, any instructions provided by Controller under Section 3.1(a) violate Applicable Data Protection Laws; and

(c) upon notice, take reasonable and appropriate steps to stop and remediate any unauthorized Processing.

3.2. Processor shall implement and maintain, at its cost and expense, appropriate technical and organizational measures in relation to the processing of Personal Data by Processor such that the Processing will meet the requirements of Applicable Data Protection Laws and ensure the protection of the rights of Data Subjects in accordance with Applicable Data Protection Laws.

3.3. Processor shall ensure a level of security in respect of Personal Data processed by it that is appropriate to the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Such measures include, without limitation, the minimum security measures specified in Annex II of Appendix 2.

3.4. Processor shall take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality.

3.5. Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties, unless Controller or this DPA specifically authorizes the disclosure, or as required by Applicable Data Protection Laws (in which case, such disclosure shall be subject to the requirements set forth in Section 4 below).

3.6. To the extent the CCPA or another U.S. state privacy law applies, Processor acts as Controller's service provider or processor and shall: (a) not Sell or Share Personal Data; (b) not retain, use, or disclose Personal Data outside the direct business relationship with Controller or for any purpose other than the specific business purposes described in the Agreement and Appendix 1, except as permitted by Applicable Data Protection Laws; (c) not combine Personal Data with personal information received from or on behalf of another person, or collected from Processor's own

interaction with a Data Subject, except as legally permitted to perform the Services; (d) comply with applicable obligations and provide the same level of privacy protection required of Controller; (e) notify Controller if Processor determines it can no longer meet those obligations; and (f) permit Controller to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data and to monitor Processor's compliance.

3.7. Processor shall not use Personal Data to train, fine-tune, evaluate, benchmark, or improve any generalized or shared artificial-intelligence or machine-learning model, or for advertising or profiling unrelated to the Services. This restriction does not prohibit Processing expressly directed or enabled by Controller for a customer-specific feature, security function, or analysis, provided the Processing remains subject to this DPA and is not used to improve a model made available to other customers.

3.8. Processor shall apply data minimization and purpose limitation to Personal Data and shall not attempt to re-identify data that Controller or Processor has de-identified, except solely to test whether de-identification processes comply with Applicable Data Protection Laws.

Section 4. Requests for Disclosure of Personal Data.

4.1. If Processor receives a request for Processing or disclosure of Personal Data (a "Disclosure Request") from a Public Authority that is located in the EEA or the United Kingdom, Processor shall promptly notify Controller of the legal or regulatory requirement and give Controller an opportunity to object to or challenge the requirement, unless Applicable Data Protection Laws prohibit such notice.

4.2. Without prejudice to the applicable SCCs, if Processor receives a Disclosure Request from a public authority that is not located in the EEA or United Kingdom, it will:

(a) assess, on a case-by-case basis, whether the Disclosure Request is legally valid, binding, and proportionate; challenge the request where there are reasonable grounds to do so; and seek interim measures where appropriate;

(b) promptly (i) notify Controller, (ii) provide reasonably available information concerning the request, and (iii) give Controller a reasonable opportunity to object or seek protective measures, unless legally prohibited; and

(c) disclose only the minimum amount of Personal Data legally required and document the request, its legal assessment, the response, and any challenge, to the extent permitted by law.

4.3. Upon written request from the Controller (email sufficing), Processor shall also provide regular updates to Controller concerning all requests for disclosure of data from Public Authorities specific to the Services being provided to Controller. These updates shall include relevant information, including, without limitation, the number of requests, type of data requested, requesting authority/ies, whether requests have been challenged, and the outcome of such challenges.

Section 5. Data Subject Rights and Assistance with Compliance.

5.1. Processor shall:

(a) promptly record and notify Controller if it receives a Data Subject Request (within three (3) business days of receipt of the request), and such notice shall provide the name and contact information of the applicable Data Subject and the details of the request;

(b) promptly record and, unless prohibited by Applicable Data Protection Laws, promptly notify Controller if it receives a Complaint (within three (3) business days of receipt of the Complaint) and, unless prohibited by Applicable Data Protection Laws, provide Controller with full details of such Complaint, including the name and contact details of the complainant;

(c) unless prohibited by Applicable Data Protection Laws, not respond to a Data Subject Request or Complaint without Controller's prior written consent;

(d) unless prohibited by Applicable Data Protection Laws, provide such information and cooperation to Controller and take such action as Controller reasonably requests in relation to each Data Subject Request or Complaint; and

(e) upon Controller's request, Processor shall provide reasonable assistance to Controller to facilitate such Data Subject Request to the extent able and in accordance with Applicable Data Protection Laws.

5.2. Processor shall, taking into account the nature of Processing and the information available to Processor, provide information, cooperation, and such other assistance to Controller as Controller reasonably requests to ensure compliance with Controller's obligations under Applicable Data Protection Laws with respect to:

(a) Data protection impact assessments (including any prior consultation required by Article 36 of the GDPR (or equivalent provision of Applicable Data Protection Laws));

(b) Notifications to any Supervisory Authority under Applicable Data Protection Laws and/or responses to Data Subject Requests or communications to Data Subjects in response to any Security Incident;

(c) Security of processing; and

(d) Any remedial action to be taken in response to any Security Incident and/or Complaint, including (subject in each case to Controller's prior written authorization) regarding any notification of a Security Incident to Supervisory Authorities and/or communication to any affected Data Subject.

Section 6. Sub-Processing.

6.1. Controller grants Processor general written authorization to engage Affiliates and third parties as Sub-processors to support the Services. The Sub-processors authorized as of the Effective Date are listed in Annex III of Appendix 2.

6.2. At any time during the term of the Agreement, Controller may request from Processor a list of Sub-processors which Processor shall provide within five (5) business days of such request.

6.3. If Processor intends on appointing a new or replacement Sub-processor, it shall notify Controller thirty (30) days prior to the date on which the proposed new or replacement Sub-processor is intended to commence its services, provided that Processor's notice to Controller may be shortened to as soon as reasonably practicable if circumstances exist, as determined by Processor in its sole reasonable discretion, that requires Processor to add or replace a Sub-processor with more immediacy to avoid material disruptions to its services and/or to avoid any further potential damages that might arise in the absence of such addition or replacement (e.g., a Security Incident at a Sub-processor). If Controller has a reasonable objection to any new or replacement Sub-processor, it shall notify Processor of such objection in writing (email sufficing) pursuant to Section 11 below, and the Parties will seek to resolve the matter in good faith. In the event Controller objects to a new Sub-processor, Processor will use reasonable efforts to make available to Controller a change in the Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Controller or adversely affecting the provision of Services to Controller. If Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Controller may terminate the Agreement and/or any order form(s) with respect to those Services which cannot be provided by Processor without the use of the objected-to new Sub-processor by providing written notice to Processor. Processor will refund Controller any unused, prepaid fees covering the remainder of the term of such Agreement and/or order form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Controller.

6.4. Processor shall engage each Sub-processor under a written agreement that imposes data-protection obligations no less protective than those imposed on Processor under this DPA, to the extent applicable to the Sub-processor's Processing, including appropriate security, confidentiality, deletion, assistance, and Restricted Transfer obligations.
6.5. Processor remains responsible for each Sub-processor's performance of its data-protection obligations to the same extent Processor would be responsible if performing the relevant Processing itself, subject to the terms of the Agreement and the applicable SCCs.

Section 7. Records and Audits.

7.1. Processor shall maintain complete, accurate and up to date written records of all categories of Processing activities carried out on behalf of Controller in accordance with Applicable Data Protection Laws, including:

(a) The categories of Processing carried out on behalf of Controller;

(b) Where applicable, details of transfers of Personal Data to recipients outside the EEA and United Kingdom; and

(c) A general description of the technical and organizational security measures referred to in Section 3.2.

7.2. Processor shall make available to Controller, upon reasonable request and within ten (10) business days, information reasonably necessary to demonstrate compliance with this DPA, including relevant records under Section 7.1, current independent audit reports or certifications, and documentation concerning applicable Transfer Mechanisms, subject to reasonable confidentiality and security restrictions.

7.3. Processor will permit Controller and its third-party representatives to audit Processor's compliance with its obligations under this DPA, on at least fifteen (15) business days' prior written notice, during the Term, provided that there shall be no more than one (1) audit per annum unless otherwise required by law. Processor will give Controller and its third-party representatives commercially reasonable assistance to conduct such audits. The assistance may include, but is not limited to: (1) physical access to, remote electronic access to, and copies of the records and any other information held at Processor's premises or on systems storing Personal Data, provided that (i) Processor shall have no such obligations with respect to Processor's cloud storage providers (e.g., AWS) that do not permit such access, and (ii) Controller shall not be provided with access to any records or information related to any third party customer of Processor and/or that does not specifically relate to Controller's data; (2) commercially reasonable access to and meetings with any of Processor's personnel reasonably necessary to provide all explanations and perform the audit effectively; and (3) inspection of all records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data, provided that Processor shall have no such obligations with respect to Processor's cloud storage providers (e.g., AWS) that do not permit such access.

7.4. The notice requirements in Section 7.3 will be reduced to five (5) business days if Controller reasonably believes that a Security Incident occurred or is occurring, or Processor is in breach of any of its obligations under this DPA or any Applicable Data Protection Laws or where the request for audit of the Processor's compliance with its obligations under Applicable Data Protection Laws and this DPA is made by a Supervisory Authority.

7.5. Processor shall promptly resolve, at its own cost and expense, all data protection and security issues discovered as a result of any audit and reported to Processor that reveal a breach by Processor of its obligations under this DPA.

7.6. If Processor is in breach of its obligations under this DPA, Controller may suspend the transfer of Personal Data to Processor until the breach is remedied. If the breach cannot be remedied within a reasonable period of time, as determined by Controller, Controller may immediately terminate the Agreement and/or any order form(s) with respect to those Services. Processor will refund Controller any unused, prepaid fees covering the remainder of the term of such Agreement and/or order form(s) following the effective date of termination with, without imposing a penalty for such termination on Controller.

7.7. Controller shall be entitled to share any notification, details, records or information provided by or on behalf of Processor with its Affiliates, professional advisors, and/or the Supervisory Authority.

Section 8. Data Transfers (Standard Contractual Clauses).

8.1. The Parties shall ensure that a valid Transfer Mechanism applies to each Restricted Transfer. Where Processor relies on certification under the EU-U.S. Data Privacy Framework or UK Extension, the SCCs and UK Addendum, as applicable, will serve as a fallback if that certification or relevant adequacy decision ceases to be valid for the transfer.

8.2. To the extent the Services involve an EEA Restricted Transfer, the Parties agree that the EEA Standard Contractual Clauses set out in Appendix 2 will apply in respect of that transfer of Personal Data. In accordance with the above:

(a) Appendix 1 shall identify whether MODULE TWO and/or MODULE THREE under the EEA Standard Contractual Clauses shall apply in respect of the transfer of Personal Data from Company (as 'data exporter') to Processor (as 'data importer').

(b) The Parties agree that "MODULE ONE" and "MODULE FOUR" under the Standard Contractual Clauses shall not apply to the Processing of Personal Data by Company or Processor.

8.3. To the extent the Services involve a UK Restricted Transfer from Company as data exporter to Processor as data importer, the UK Addendum in Appendix 3 will apply and modify the EEA Standard Contractual Clauses for that transfer.

8.4. Upon reasonable request, Processor shall provide information reasonably necessary for Controller to complete and document a transfer impact assessment under the GDPR or the data protection test/transfer risk assessment required under UK Data Protection Law, taking into account the nature of the Processing and information available to Processor.

8.5. Where any updates, new version, or amendments to, or replacement of, an existing Transfer Mechanism is approved by the competent authority/ies (including, where applicable, the European Commission, a UK Government Department or a competent regulatory authority) during the term of this DPA ("New Transfer Mechanism"), the New Transfer Mechanism will be deemed to replace the applicable Transfer Mechanism from the date on which the new Transfer Mechanism takes effect under Applicable Data Protection Laws and both Parties will take such steps as is necessary to implement and incorporate the new Transfer Mechanism, provided that if Processor is unable or unwilling, on a commercially reasonable basis, to implement and incorporate the New Transfer Mechanism, then Processor may instead provide prior written notice to Controller of same (the "Opt-Out Notice") and, in such case, either party may immediately terminate the Agreement and/or any order form(s) with respect to those Services. In such case, Processor will refund Controller any unused, prepaid fees covering the remainder of the term of such Agreement and/or order form(s) following the effective date of termination with, without imposing a penalty for such termination on Controller. Unless the Opt-Out Notice is sent by Processor, as soon as the New Transfer Mechanism takes effect, the Parties will take all steps to implement such New Transfer Mechanism, including working together to amend the DPA and its annexes to reflect the applicable changes.

8.6. Controller authorizes Restricted Transfers made to the locations and Sub-processors identified in this DPA or otherwise notified under Section 6, provided that each transfer complies with

Applicable Data Protection Laws and is covered by a valid Transfer Mechanism. Processor shall not materially change the location of Processing in a manner that creates a new Restricted Transfer without providing notice under Section 6.

(a) [Reserved.]

(b) [Reserved.]

8.7. Without prejudice to Section 6 and Section 8.2 above, if, in the performance of this DPA, Processor's Processing of Personal Data involves any Restricted Transfer (including, in respect of any EEA Restricted Transfer, onward transfer of Personal Data to a Sub-processor that is not subject to the GDPR), Processor shall in advance of any such Restricted Transfer ensure that a satisfactory Transfer Mechanism is in place.

8.8. Processor shall implement supplementary technical, contractual, and organizational measures reasonably necessary for a Restricted Transfer and shall promptly notify Controller if Processor determines it can no longer comply with the applicable Transfer Mechanism. The Parties shall cooperate in good faith to suspend the affected transfer or implement an alternative lawful mechanism.

8.9. For transfers subject to the Swiss Federal Act on Data Protection, the EEA Standard Contractual Clauses apply with the following adaptations: references to the GDPR include the Swiss Federal Act on Data Protection; references to the EU, Union, EEA, or Member State include Switzerland; the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner to the extent required; and data subjects in Switzerland may enforce their rights in Switzerland.

Section 9. Security Incident.

9.1. In respect of any Security Incident, Processor shall:

(a) notify Controller without undue delay and, in any event, within forty-eight (48) hours after becoming aware of a Security Incident;

(b) not make any public announcement about a Security Incident (a "Breach Notice") without the prior written consent of Controller, unless required by Applicable Data Protection Laws;

(c) provide the information required by Article 33(3) of the GDPR and other Applicable Data Protection Laws as it becomes available, including the nature and likely consequences of the Security Incident, affected categories and approximate volumes of Data Subjects and records, mitigation and remediation measures, and a contact for follow-up; and provide regular material updates until containment and remediation are complete;

(d) promptly investigate, contain, mitigate, and remediate the Security Incident; preserve relevant evidence; reasonably cooperate with Controller's investigation and legally required notifications; and provide, upon request, a written root-cause and corrective-action summary when the investigation is complete. Notification of a Security Incident is not an admission of fault or liability.

Section 10. Term. This DPA will remain in full force and effect so long as: (A) the Agreement remains in effect, or (B) Processor retains any Personal Data related to the Agreement in its possession or control ("Term").

Section 11. Required Notices. All notices required to be provided to Controller under this DPA shall be sent to the Controller in accordance with the notice provisions of the Agreement. All notices required to be provided to Processor under this DPA shall be sent via email to the email to compliance@ninjio.com, with a copy sent by overnight courier services to: Ninjio, LLC, 880 Hampshire Road, Suite B, Westlake Village, CA 91361, Attention: Legal Department (Privacy).

Section 12. Deletion or Return of Personal Data and Copies.

12.1. At Controller's choice, Processor shall securely return or delete Personal Data within thirty (30) days after termination or expiration of the Services involving that Personal Data, or earlier upon Controller's documented request where the Personal Data is no longer required to provide the Services, unless retention is required by Applicable Data Protection Laws. Processor may retain Personal Data that remains in secure backups until deleted in accordance with its ordinary backup lifecycle, provided that the data is isolated from further Processing except for security, disaster recovery, or legal compliance.

12.2. If any Applicable Data Protection Laws requires Processor to retain any documents or materials that Processor would otherwise be required to return or destroy, it will notify Controller in writing of that retention requirement (to the extent permitted under applicable law), giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.
12.3. Upon written request, Processor shall provide written confirmation that return or deletion has been completed in accordance with this Section 12. Any restored backup containing Personal Data remains subject to this DPA and shall be deleted or placed beyond use after the restoration purpose is complete.

Section 13. General.

13.1. Except as expressly required under the applicable Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the Parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

13.2. Subject to the Standard Contractual Clauses, this DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflicts of laws principles. The Parties consent to the personal jurisdiction of, and venue in, the courts of Los Angeles, California.

13.3. This DPA is the final, complete, and exclusive agreement of the Parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. No modification of, amendment to, or waiver of any

rights under the DPA will be effective unless in writing and signed by an authorized signatory of each Party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each Party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such Party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such Party, enforceable in accordance with its terms.

13.4. The order of precedence is: (a) the applicable SCCs or UK Addendum, but only with respect to the Restricted Transfer they govern; (b) this DPA; and (c) the Agreement. Nothing in the Agreement or this DPA varies or contradicts the SCCs or prejudices the fundamental rights or freedoms of Data Subjects.

WHEREOF, the Parties by their duly authorized representatives, have executed this DPA as of the date(s) set forth below, the latter of which shall be the effective date of this DPA ("Effective Date").

Ninjio, LLC "Processor"	**Company:**_____ "Controller"
By:	By:
Name:	Name:
Title:	Title:

Appendix 1: Personal Data Processing Purposes And Details

1. **Categories of data subjects whose personal data is processed**

   Company's Authorized Users and administrators (as defined in the Agreement), including employees, contractors, and other individuals whom Company authorizes to participate in or administer the Services.

2. **Categories of personal data processed**

   Account and profile data (such as name, business email address, employee or user identifier, job title, phone number, company, department, manager, branch, location, and other customer-configured attributes); authentication and provisioning data; IP address, device, operating-system, and browser data; training assignment, completion, quiz, and engagement data; phishing-simulation interaction and reporting events; risk, susceptibility, and program-performance metrics derived from use of the Services; support communications; and other Personal Data submitted or configured by Company for the Services. Processor does not require government identifiers, financial-account credentials, health data, or other Sensitive Personal Data for the Services.

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

   No Sensitive Personal Data is intended or required to be Processed. Controller shall not submit Sensitive Personal Data unless expressly agreed in writing and supported by appropriate safeguards.

4. **Subject matter and nature of the processing**

   The Processing includes collection, transmission, storage, organization, retrieval, analysis, generation of customer-specific risk and program metrics, support, security monitoring, backup, deletion, and other operations necessary to provide, secure, maintain, and improve the Services for Company in accordance with Controller's instructions.

5. **Purpose(s) for which the personal data is processed on behalf of the Controller**

   To provide and administer cybersecurity awareness training, phishing and social-engineering simulations, user and administrator portals, program reporting and analytics, customer-configured risk and personalization features, support, security, fraud prevention, troubleshooting, and related Services described in the Agreement.

6. **Duration of the processing**

Personal Data will be Processed for the term of the applicable Services and thereafter only as permitted by Section 12, including the ordinary backup lifecycle and any legally required retention.

7. Applicable Module(s) for the Standard Contractual Clauses

Check All that Apply with 'XX'	**Applicable Module**
XX	**MODULE TWO**: The Parties have selected "MODULE TWO" under the EEA Standard Contractual Clauses in respect of the transfer of Personal Data from Company (as 'data exporter') to Processor (as 'data importer') where Company acts as a Data Controller, and Processor acts as a Data Processor.
XX	**MODULE THREE**: The Parties have selected "MODULE THREE" under the EEA Standard Contractual Clauses in respect of the transfer of Personal Data from Company (as 'data exporter') to Processor (as 'data importer') where Company acts as a Data Processor to its end user business clients (where such clients are the Data Controller) pursuant to the instructions of these Data Controller-clients, and Processor acts as a sub-processor.

APPENDIX 2

2021 EU Model Clauses extracted from the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 Annex on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

---

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

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

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

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

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

Clause 2

Effect and invariability of the Clauses

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

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

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

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

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

8.2 **Purpose limitation**

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

8.3 **Transparency**

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

8.4 **Accuracy**

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

8.5 **Duration of processing and erasure or return of data**

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

8.6 **Security of processing**

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

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

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

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

8.7 **Sensitive data**

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

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

8.9 **Documentation and compliance**

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([3]).

8.2 **Purpose Limitation**

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

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information

8.4 **Accuracy**

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

8.5 **Duration of processing and erasure or return of data**

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

8.6 **Security of processing**

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

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

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

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

8.7 **Sensitive data**

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

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 **Documentation and compliance**

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

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

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

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

Clause 9

Use of sub-processors

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([5]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([6]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

---

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 12

Liability

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and

freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([7]);

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

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

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

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

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

Clause 15

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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

15.1 **Notification**

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

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

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

[***For Module Three***: The data exporter shall forward the notification to the controller.]

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

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

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

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

15.2 **Review of legality and data minimisation**

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority [***for Module Three***: and the controller] of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

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

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

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

Annex I

A. LIST OF PARTIES

MODULE TWO AND MODULE THREE (as applicable)

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

1. Name:

   Address:

   Contact person's name, position and contact details:

   EU GDPR Representative:
   Name:
   Address:
   Contact person's name, position and contact details:
   Email:

   Activities relevant to the data transferred under these Clauses: Data exporter's receipt of the Services described in the Agreement.

   Signature: _____ Dated: _____

   Role: Controller for Module Two; Processor acting on behalf of its controller customer(s) for Module Three.

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

1. Name: Ninjio, LLC

   Address: 880 Hampshire Road, Suite B, Westlake Village, CA 91361

   Contact person's name, position and contact details: Laura Bell Main (CTO) lmain@ninjio.com and compliance@ninjio.com.

   Activities relevant to the data transferred under these Clauses: Data importer's provision of the Services described in the Agreement

   Signature: _____ Dated: _____

   Role: Processor for Module Two; Sub-processor for Module Three.

B. DESCRIPTION OF TRANSFER

MODULE TWO AND MODULE THREE (as applicable)

1. **Categories of data subjects whose personal data is transferred**

   Company's Authorized Users and administrators, including employees, contractors, and other individuals whom Company authorizes to participate in or administer the Services.

2. **Categories of personal data transferred**

   The categories of Personal Data described in Appendix 1, Section 2, which is incorporated into this Annex I.B.

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

   No Sensitive Personal Data is intended or required to be transferred. The restrictions and safeguards in Appendix 1, Section 3 apply.

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

   Continuous or periodic, depending on Company's provisioning, configuration, and use of the Services, for the duration of the applicable Services.

5. **Nature of the processing**

   The Processing will comprise the Processing necessary to provide the Services to data exporter pursuant to the Agreement.

6. **Purpose(s) of the data transfer and further processing**

   The purposes described in Appendix 1, Section 5, which is incorporated into this Annex I.B.

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

   The retention period and criteria described in Appendix 1, Section 6 and Section 12 of the DPA.

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

   As per Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO AND MODULE THREE (as applicable)

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

The supervisory authority determined in accordance with Clause 13 of the applicable SCC Module, based on the data exporter's establishment, representative, or affected Data Subjects. Where Ireland is the competent Member State, the authority is the Data Protection Commission.

Annex II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL
MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO AND MODULE THREE (as applicable)

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.
Processor shall maintain the measures in this Annex II and may update them to reflect technical progress, provided that no update materially decreases the overall security of the Services during the Term. The measures shall include, as appropriate to the risk: encryption in transit and at rest; least-privilege access and multifactor authentication; logging and monitoring; secure software development and change control; vulnerability management and independent testing; incident response; personnel confidentiality and security training; vendor risk management; backup and business continuity; and processes for deletion, restoration, and assistance with Data Subject rights.

Information Security Policy

Executive Summary

NINJIO's Commitment to Cybersecurity & Data Protection

At NINJIO, our commitment to cybersecurity is unwavering. Recognizing the immense responsibility of safeguarding our digital ecosystem and the sensitive data of our clients, we've made it our top priority to establish and maintain a robust cybersecurity infrastructure. Our foundation is built on a culture of security awareness, where every team member understands the role they play in fortifying our digital defenses.

Central to our cybersecurity strategy is the alignment with globally recognized best practices frameworks. By rigorously adhering to the guidelines and controls set forth by NIST, ISO, and SOC, we ensure a comprehensive and multi-faceted approach to security. These frameworks guide our initiatives, from risk management and system hardening to access control and incident response. The result is a resilient infrastructure capable of defending against both current and emerging threats.

Beyond mere compliance, we believe in the power of evolution. As the digital landscape continuously transforms, so too does the nature of cyber threats. In this context, a static approach to cybersecurity is insufficient. Our dedication to continuous learning, regular system audits, and proactive threat hunting allows us to stay ahead of potential vulnerabilities. By investing in the latest technologies and cybersecurity training, we ensure that our defenses remain agile and adaptive.

The protection of client data is more than just a mandate; it's a covenant we hold sacred. Our clients entrust us with their information, expecting not just confidentiality, but also integrity and availability. We work tirelessly to exceed these expectations, applying layers of encryption, redundant backups, and stringent access controls to safeguard their data.

NINJIO's commitment to cybersecurity is all-encompassing. It's a blend of adherence to the best global standards, an unwavering commitment to our clients, and an ever-evolving approach to asset protection.

Physical Controls:

Datacenter Physical Location: AWS Seattle, US - Zone Name: us-west-2-sea-1a - Parent Region: US West (Oregon)

Secure Data Centers: Our servers are hosted in state-of-the-art data centers with rigorous access controls, including 24/7 monitoring, video surveillance, biometric access, and on-site security personnel.

Physical Access Records: Records of physical access to our facilities are maintained and regularly reviewed.

Equipment Protections: All equipment is safeguarded against potential environmental threats, such as floods or fires.

Technical Controls:

Regular Vulnerability Assessments: Our platform undergoes regular vulnerability assessments and penetration tests.

Identity and Access Management: We utilize multi-factor authentication and least privilege access principles to ensure that only authorized individuals can access sensitive systems.

Continuous Monitoring: Our systems are continuously monitored for anomalies or suspicious activities.

Network Security: Our network is protected with advanced firewall systems, intrusion detection and prevention systems (IDPS), and other protective measures.

User Responsibilities: Our platform mandates robust password policies, and we emphasize the importance of secure authentication methods, including the use of two-factor authentication where critical.

Cryptography:

Data at Rest Encryption:

Comprehensive Coverage: All sensitive data stored in our databases, file systems, and storage infrastructures is encrypted, irrespective of its format or type.

Advanced Encryption Standards (AES): We utilize AES-256, a recognized industry standard, to encrypt our data at rest, ensuring high levels of confidentiality and security.

Key Management: Our encryption keys are securely managed and stored in separate environments from the data they protect. We also practice regular key rotations, reducing the risk of any potential compromise.

Regular Audits: Periodic security audits ensure that our encryption measures remain robust, and any potential vulnerabilities are swiftly addressed.

Data in Transit Encryption:

TLS/SSL Protocols: All data transferred to and from our systems is secured using TLS (Transport Layer Security) or its predecessor, SSL (Secure Sockets Layer). This ensures that any data in transit remains private and integral.

End-to-End Encryption: For especially sensitive data transfers, we utilize end-to-end encryption, ensuring that data remains encrypted from the point of origin to its intended destination without any intermediary decryption.

Perfect Forward Secrecy (PFS): Our systems support PFS, which ensures that even if encryption keys are compromised, historical communication remains secure and inaccessible.

Monitoring and Alerts: Automated monitoring tools oversee our data transfer channels for any signs of unusual or potentially malicious activity, allowing us to respond proactively to any potential threats.

Network Security Management:

Network Controls: Our network infrastructure uses advanced firewall systems, intrusion detection mechanisms, and strategic network segregation to ensure optimal security.

Security of Network Services: We keep our network services updated with the latest security patches and maintain secure configurations to minimize vulnerabilities.

Information Transfer:

Data Transfer Policies: We've put in place strict guidelines and technologies ensuring secure data transfer, be it electronic or physical.

Email Security: Our platform utilizes email security solutions to guard against malicious content and unauthorized data dissemination. Allow listing, dedicated sending IP's, SPF, DMARC, and DKIM are incorporated for best practices email security.

Operating System Security:

Malware Protection: We're vigilant about potential threats. Our anti-malware solutions are always updated and active, offering real-time protection.

Backup: We perform regular encrypted backups of essential data and frequently test our backup restoration processes to ensure data resilience.

Logging and Monitoring: Our platform is designed to continuously capture, store, and analyze logs, with real-time alerts set up for critical events.

System Hardening:

Baseline Configurations: All our systems are deployed with a secure baseline configuration, eliminating unnecessary services, accounts, and functionalities that might pose potential vulnerabilities.

Patch Management: We prioritize timely updates and patches. As soon as a security patch is available, we evaluate, test, and deploy it to mitigate potential vulnerabilities.

Reduced Surface Area: By turning off unused and unnecessary services, protocols, and ports, we minimize the potential entry points for attackers.

Security Configurations: From file permissions to firewall settings, we employ rigorous configurations to ensure that only legitimate users and processes can access our systems.

Continuous Monitoring: Our systems are continuously monitored to detect and alert against any configuration drifts, ensuring we maintain our hardened posture consistently.

Authorized Application Control:

Allowlisting: Instead of merely blocking harmful applications, we employ an application allowlisting approach. This ensures that only pre-approved and verified applications can execute on our systems.

Regular Reviews: The list of authorized applications is reviewed periodically. Old applications that are no longer in use or have become redundant are promptly removed.

Behavior Analysis: Advanced behavioral analysis tools monitor our applications for any deviations from their regular operational patterns, which could indicate potential threats or compromises.

Integration with Threat Intelligence: Our application control solutions are integrated with threat intelligence platforms, providing real-time data about emerging threats and allowing us to react proactively.

User Access Controls: Even authorized applications have layered access controls, ensuring that users can only access functionalities relevant to their roles and responsibilities.

Access Control and User Management:

Least Privilege Access:

Role-Based Access Control (RBAC): We utilize RBAC to ensure users are granted only the permissions essential to perform their designated roles. This minimizes potential vectors for unauthorized data access or manipulation.

Systematic Review: Periodically, we reassess the access levels of all users to ensure they align with current job functions and responsibilities.

Regular Auditing of Privileged Accounts:

Scheduled Audits: Privileged accounts, due to their elevated access, are subject to frequent and rigorous audits. This helps us ensure that such accounts are not misused or compromised.

Real-time Monitoring: We employ automated systems to monitor the activities of privileged accounts in real time, triggering alerts for any unauthorized or suspicious actions.

Separation of Duties: To further mitigate risks, we ensure that high-level privileges are divided among multiple roles, preventing any single account from having excessive system access.

Unique User Policy:

Unique Identifiers: Every user in our system, regardless of their role, is assigned a unique identifier. This ensures that all actions can be accurately traced to an individual, promoting accountability and transparency.

Authentication Measures: To ensure the security of unique user accounts, we employ robust authentication mechanisms, including strong password policies and multi-factor authentication where appropriate.

Termination and Transitions: Upon an employee's departure or role transition, we have procedures in place to promptly modify or revoke their access, ensuring it aligns with their new status or role.

Application Security:

Systematic Approach to SDLC:

Requirement Analysis: Before any code is written, we invest time in understanding the precise needs of our users and stakeholders. This ensures the solutions we develop are not just technically sound but also truly resonate with our users' needs.

Design and Architecture: We prioritize scalable and modular designs, ensuring our platform remains adaptable to future requirements and technological changes.

Implementation: Our developers, armed with a clear roadmap, harness the latest tools and methodologies to bring our designs to life.

Testing: Rigorous testing phases, including unit, integration, system, and user acceptance testing, ensure our software meets the highest standards of reliability and performance.

Deployment: We follow a structured deployment process, often leveraging automated CI/CD pipelines, to ensure smooth rollouts.

Maintenance: Continuous monitoring and feedback loops ensure our platform evolves, remains up-to-date, and always delivers peak performance.

Secure Code Development:

Security Training: Our developers undergo regular training on the latest security threats and best practices, ensuring security is top of mind during code creation.

Secure Coding Standards: We adhere to recognized secure coding standards, minimizing common vulnerabilities like SQL injection, cross-site scripting, and buffer overflows.

Code Reviews: Every piece of code undergoes peer reviews, ensuring another set of eyes verifies its integrity and security.

Static and Dynamic Analysis: We employ automated tools to scan our codebases for potential vulnerabilities, ensuring they're addressed before going into production.

Penetration Testing: Periodic penetration tests challenge our platform's defenses, helping us identify and rectify potential weak points.

Patch Management: We maintain a structured process for identifying, prioritizing, and implementing security patches, ensuring our platform remains resilient against known vulnerabilities.

Administrative Controls:

Employee Training: All stakeholders, including employees and contractors, undergo security awareness programs to instill a culture of security. We ensure that all our employees are regularly trained on the best practices of data handling, privacy, classification, and security.

Risk Assessment: Periodic risk assessments ensure that we identify, assess, and mitigate risks.

Security Policies and Procedures: We maintain comprehensive security policies and procedures that are aligned with best practices cybersecurity frameworks such as NIST and ISO recommendations.

Incident Response: Our incident response team is always ready to handle potential security threats, ensuring quick mitigation and resolution.

Internal Audits: We conduct internal audits regularly.

Service Operations Change Management:

Change Advisory Board (CAB):

We've instituted a Change Advisory Board (CAB) that comprises cross-functional team members. This board reviews and approves significant changes, ensuring they align with our platform's objectives and do not disrupt the user experience.

Formal Change Requests:

All changes, regardless of their size or impact, start with a formal change request. This standardized approach ensures that every change is documented, traceable, and managed systematically.

Impact Analysis:

Before implementing any change, we conduct a comprehensive impact analysis. This helps us understand potential ramifications, dependencies, and risks, allowing us to prepare effectively.

Change Testing and Validation:

Once a change is approved, it's rigorously tested in a controlled environment to ensure it functions as intended and doesn't introduce new vulnerabilities or issues.

Scheduled Rollouts:

We understand the value of our users' time. Hence, major changes are scheduled during off-peak hours or times when platform usage is at its lowest, ensuring minimal disruption.

Rollback Plans:

While we take every precaution to ensure changes are successful, we're also prepared for unforeseen challenges. Every change is accompanied by a detailed rollback plan to restore services to their prior state if needed.

Communication and Transparency:

Communication is paramount. We inform our users of significant upcoming changes, any expected downtime, and the benefits the changes will bring. This ensures that they're not caught off guard and can plan their activities accordingly.

Post-Change Review:

After each significant change, we conduct a post-implementation review. This helps us assess the effectiveness of the change, gather feedback, and continuously refine our change management processes.

Continuous Training and Awareness:

Our team undergoes regular training on change management best practices. We believe that a well-informed team is the first step to implementing changes seamlessly.

We remain committed to continuously advancing our security posture and ensuring that we provide a secure and resilient SaaS platform for our clients. For more detailed information on our security practices or specific certifications, please contact our security team.

Hiring and HR Practices:

At NINJIO our most valued assets are our employees. To ensure the trust and security that our clients, partners, and stakeholders expect from us, we've put in place rigorous hiring practices, especially with regard to background checks. Our processes are meticulously designed to align with internationally recognized standards, including ISO, NIST, and SOC. Here’s how we prioritize integrity and trust in our hiring process:

Comprehensive Background Checks:

Criminal Records: We conduct thorough criminal record checks for every potential hire. This helps us ensure that the individuals joining our team have a history consistent with our company values and the trust placed in us by our clients.

Employment and Education Verification: We verify the employment and educational history of all potential hires, ensuring their qualifications and experiences align with what's presented to us.

Reference Checks: Reaching out to listed references provides us additional insights into a candidate's professional conduct and capabilities.

Alignment with Recognized Standards:

ISO Standards: Our hiring processes and data handling during the recruitment phase comply with ISO standards, ensuring personal data protection and procedural integrity.

NIST Guidelines: In line with NIST guidelines, we maintain a systematic and consistent approach to evaluating the trustworthiness and suitability of candidates, especially those for roles with significant responsibilities.

SOC Protocols: As part of our commitment to transparency and process reliability, our background check processes are designed to be verifiable and auditable, consistent with SOC protocols.

Privacy and Consent:

Informed Consent: Before conducting any background checks, we obtain clear and informed consent from the potential hire. We believe in transparency and ensure candidates understand the purpose and extent of the checks.

Data Privacy: Respecting the confidentiality and privacy of candidate information is paramount. All personal data gathered during the hiring process is handled and stored with the utmost care, in line with data protection regulations and best practices.

Continuous Training for HR:

Our HR team undergoes regular training on the latest in hiring best practices, standards, and regulations, ensuring our processes remain up-to-date, fair, and reliable.

Incident Response Procedures in Compliance with GDPR and CCPA/CPRA

Proactive Detection

Our state-of-the-art monitoring tools are always on the alert, scanning our systems for irregularities or malicious activities, ensuring early detection of potential data breaches.

Structured Response

Every detected incident activates a well-defined protocol — from identifying and containing the threat, both short-term and long-term, to its eradication, system recovery, and the subsequent reflective phase of drawing lessons from the event.

Communication Protocols in line with GDPR and CCPA/CPRA:

Notification to Authorities: In accordance with GDPR, in the event of a personal data breach, we will notify the appropriate supervisory authority within 72 hours of detection, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. For breaches falling under CCPA/CPRA, we adhere to the stipulated notification timelines and guidelines.

Notification to Data Subjects: Where a breach is likely to result in high risk to the rights and freedoms of individuals, under GDPR, we will communicate the breach to the affected data subjects without undue delay. Similarly, CCPA/CPRA provisions guide our communication to California residents.

Continuous Learning & Regulatory Reporting

Post-incident evaluations are standard procedure. Besides gleaning learnings to prevent future breaches, these evaluations also inform any necessary updates to our routine reports to supervisory authorities, ensuring compliance with ongoing GDPR and CCPA/CPRA requirements.

Collaboration with Legal and Regulatory Experts

Recognizing the nuanced and evolving nature of data protection regulations, we collaborate with legal and regulatory experts to ensure that our incident response procedures remain compliant with GDPR, CCPA/CPRA, and other relevant regulations.

Employee Training & Awareness

Regular training sessions familiarize our team with the latest in cybersecurity and regulatory requirements. This ensures swift, decisive, and compliant action during incidents.

Cybersecurity and Compliance Technical Tables

GDPR

Question #	Question	Response	Additional Comments
GDPR-1	Does your organization comply with industry standards? (For example, Information Security (e.g. ISO 27001), Environmental Management (e.g. ISO 14001), Quality Management (e.g. ISO 9001), PCI DSS etc.)	Yes	NINJIO holds a SOC 2 Type 2 report covering the Security trust services criteria for the NINJIO Commercial Platform, for the period 1 April 2026 to 30 June 2026, issued by Insight Assurance. The report is available to customers and prospective customers under NDA through the NINJIO Trust Center at trust.ninjio.com.
GDPR-2	Do you have an identified senior representative who has overall responsibility for data protection matters within your organization? If so, provide details	Yes	Email: _compliance@ninjio.com Laura Bell Main - CTO
GDPR-2.1	Does your organization have documented data protection and information security policies and procedures? If so, please share	Yes	Included: 1.1 Personal Data Protection Policy https://ninjio.com/privacy
GDPR-2.2	Have you recently conducted an audit of those policies and procedures?	Yes	
GDPR-2.3	Have customers raised data protection concerns with your organization?	No	
GDPR-2.4	Does your organization ensure that all individuals who will be processing Personal Data undergo training in relation to data protection awareness and the handling of Personal Data?	Yes	Monthly + Annual Training
GDPR-2.5	Is a detailed explanation of the technical and security measures which your organization takes to protect the integrity of customer Personal Data available? If so, please share	Yes	Included

GDPR-2.6	Is customer information stored in encrypted form, or is the data tokenized?	Yes	Encryption at Rest and in Transit
GDPR-2.7	Has your organization ever been (i) subject to a complaint in relation to data protection from either an individual or the applicable data protection regulatory body or (ii) reported a data breach?	No	
GDPR-2.8	Has your organization ever reported a data breach to an individual or the applicable data protection regulatory body?	No	
GDPR-2.9	Does your organization have a contingency plan to manage the consequences of an unforeseen event that might affect Personal Data?	Yes	
GDPR-2.10	Is personal information or log-on credentials stored in the cloud?	Yes	We store non-sensitive PII such as name, email address and department for the purpose of security awareness training and reporting. We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash.
GDPR-2.11	In which jurisdiction is the data stored?	N/A	United States
GDPR-2.12	Will your organization utilize subcontractors in the provision of the solution/services? If yes, provide details	Yes	See DPA for list of Subprocessors
GDPR-2.13	Does Vendor have the ability to access, update, retrieve (in a usable format), block, share in a portable format, or delete all Personal Data, including on termination of the services?	Yes	https://ninjio.com/privacy
GDPR-2.14	Are audit trails are in place to enable you to monitor who is accessing the Personal Data?	Yes	
GDPR-2.15	Can your company restore Personal Data (without alteration) from a back-up if it suffered a major data loss within 24 hours?	Yes	

In-Scope Personal Data

Personal Data Scope	NINJIO Standard
Provide a summary of the specific services to be performed by each party, which will assist in determining whether the roles are controller or processor:	NINJIO provides security awareness training through a hosted platform. Client is responsible for exporting employee data to the platform for the purpose of security awareness testing and training. The NINJIO platform stores data related to the ongoing program for reporting purposes on training and testing outcomes.
List the specific data elements in scope (for example, names, addresses, email, geolocation information, etc.) that each party will provide or make available to the other party in connection with the contemplated product or service:	Non-sensitive employee data. At a minimum, NINJIO requires a first and last name, and an email address to deliver services. Client may add additional attributes to enhance reporting, such as: department, location, manager, employee ID, title, phone number, etc. NINJIO also stores results related to training and testing interactions and stores IP, browser and OS attributes for these interactions.
List the specific locations or countries from where the personal data originates (for example, US, UK, EU, etc.)	Data is stored and processed in the U.S.
Indicate all of the applicable personal data transfers between the parties in scope of the engagement (for example, UK to EU, US to UK, UK to US, EU to US, etc.) and include any locations where data will be stored, processed, or used in connection with the contemplated product or service:	Data is stored and processed in the U.S.

Data Protection and Access Controls

Data Classification

NINJIO's data classification matrix including data definition, access restrictions and minimum controls specific for your service	See Data Classification Matrix

Data Access and Handling

Describe how your organization decides who does and does not have access to sensitive data	Least Privilege Access Policy
Data Anonymization	See Data Anonymization Attachment
NINJIO's general rules management in relation to role provisioning, deprovisioning, and recertification.	See Change Management.

Which groups of staff (individual contractors and full-time) have access to personal and sensitive data handed to you?	Support Staff/Tech Ops Management - Trained and responsible for managing services.
Do you keep sensitive data (as defined by your data classification matrix) in hard copy (e.g. paper copies)? If so, please describe.	No. NINJIO only stores non-sensitive PII in digital format and does not store hard copies.
Do you have a procedure for securely destroying hard copy sensitive data?	N/A
Do you support secure deletion (e.g. degaussing/cryptographic wiping) of archived or backed-up data?	Yes. See Data Destruction Policy
Describe the circumstances in which customer data is allowed leave your production systems?	Only at the request of the data controller

Authentication

Do you have an internal password policy?	Yes
Do you have complexity or length requirements for passwords?	Yes
How are passwords hashed?	We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash. We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash.
Do employees/contractors have ability to remotely connect to your production systems? (i.e. VPN)	Only Privileged users have VPN access, which requires 2FA and is on a DMZ with stateful packet inspection.
Is MFA required for employees/contractors to log in to production systems?	2FA is required for employees accessing all systems containing client personal data.
Do internal applications leverage SSO for authentication?	Yes

Third Party Data Processing

Which processors (vendors) access your customer's information?	See DPA for list of 3rd party sub-processors and details.
Do these processors (vendors) contractually comply with your security standards for data processing?	Yes
How do you regularly audit your critical vendors?	Security Assessments

Policies and Standards Management Program

Do you have a formal Information Security Program (InfoSec SP) in place?	Yes
Do you review your Information Security Policies at least once a year?	Yes
Do you have a Information security risk management program (InfoSec RMP)?	Yes
Do you have management support or a security management forum to evaluate and take action on security risks?	Yes
Do you have a dedicated information security team?	Internal and Outsourced: MSSP

Policy Execution

Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?	Yes
Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes

Proactive Cybersecurity

Independent 3rd Party Penetration Testing

How is your network security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology	Internal Resources: Monthly & Annually. Independent 3rd Party Auditors: Annual Commercial Systems Penetration test Annual Production Systems Internal/External Penetration test
How is your application security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology	Independent 3rd party testing. See appendix for (most recent) Platform Penetration Test Results

Vulnerability Management/Patching

Network vulnerability management processes and procedures	Monthly vulnerability scanning and patch management is performed. Critical vulnerabilities are addressed out of band and urgently scoring a 7 or higher on the CVSS score rating system.
Timeframe for patching critical vulnerabilities	Critical Vulnerabilities follow emergency change management protocols which is described under change management policies.
Vulnerability management tools	Rapid7 Nexpose & Microsoft Defender

Application Vulnerability Management	
Please summarize or attach your application vulnerability management processes and procedures?	Monthly Scans and remediation as needed.
What tools do you use for application vulnerability management?	Rapid7 Nexpose – M365 Defender
Production Patching	
How do you regularly evaluate patches and updates for your infrastructure?	Monthly
Responsible Disclosure	
Do you publish a path for responsible disclosure of security vulnerabilities (ie security@ or /security)?	No
Do you have an established bug bounty program?	No

Endpoint Security

Are all endpoint laptops that connect directly to production networks centrally managed?	Yes
Describe standard employee issued device security configuration/features.	Login Password, antimalware, EDR, full disk Encryption, administrative privileges locked, firewall, application allow-listing, OS and service hardening, auto-lock, denied removable storage, agent-based vulnerability scanning, content filtering, automatic quarantine upon detected incident.
Does sensitive or private data ever reside on endpoint devices? How is this policy enforced?	No. managed by administrative policy and technical controls.
How do you limit data exfiltration from production endpoint devices?	DLP rules aligned to PCI/HIPAA/GDPR/PII, and technical controls for commercial system export policies.
What systems do you have in place that mitigate classes of web application vulnerabilities? (e.g.: WAF, proxies, etc)	WAF (Q4 2024)
Do you have breach detection systems and/or anomaly detection with alerting?	Yes – Microsoft Defender & Huntress + Network/Device IPS & SIEM

Infrastructure Security

Config Management	
Are the hosts where the service is running uniformly configured?	Yes
Are changes to the production environment reviewed by at least two engineers/operations staff?	Yes
Secrets Management	
Describe your secrets management strategy:(auth tokens, passwords, API credentials, certificates)	We store administrative credentials in the platform using best practice standards by using

	PBKDF2 algorithm withing SHA256 hash. We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash.
Logs	
Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?	Yes
Network Security	
Is the production network segmented in to different zones based on security levels?	Yes
What is the process for making changes to network configuration?	See Change Management Procedure.
Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (TLS, VPN, IPSEC, etc).	Yes

Application Security: Customer Facing

Authentication	
Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options	SSO is not supported at this time. We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash. We store administrative credentials in the platform using best practice standards by using PBKDF2 algorithm withing SHA256 hash.
Does application allow user MFA to be enforced by admins?	No
Does application support IP whitelisting for user authentication?	No
Role Based Access Control	
Does your application support standardized roles and permissions for users (ie admin, user)?	Yes
Does your application enable custom granular permissions and roles to be created?	Yes (limited)
Audit logging	
Which audit trails and logs are kept for systems and applications with access to customer data?	
Does your application provide customer adminstrators with direct access to verbose audit logs (API, export, viewer etc)?	No
Data Retention	
Does your application allow for custom data retention policy for customer data?	No

Change management	
Does your application provide a change log?	Yes
Does your application provide a sandbox environment to customers for testing?	Available upon request. A separate environment may involve additional fees.
API Management	
Does your API implement rate limiting?	N/A
How does your application store API keys?	N/A
Does application support IP whitelisting for API access?	N/A

Measures for Fulfilling Data Subject Rights Request

Company can send these requests to compliance@ninjio.com.

Annex III
LIST OF SUB-PROCESSORS

MODULE TWO AND MODULE THREE (as applicable)

Name	Phone	Address	Services/Sub-Processing Activities
ConnectWise, LLC	813.463.4700	400 N Tampa St, Suite 130 Tampa, FL 33602, USA	Billing PII, Company and Employee PII, Family Use Rights PII, Support related activities
HubSpot, Inc.	888 482 7768	2 Canal Park Cambridge, MA 02141	Company and user details, pre and post sale, email interactions
Microsoft Corp	(425) 882 8080	1 Microsoft Way Redmond, WA, 98052	Email, productivity: word, excel, powerpoint, outlook - stored in sharepoint & exchange online, Friends and Family Use Rights. Client Sign-up for adding Friends and family members to Ninjio. First name and email address only. Consent for minors. Data is sent encrypted to ConnectWise where stored and processed. Data is not stored on Azure platform after processing
Amazon Web Services, Inc.	AWS General Counsel, privacyshield@amazon.com	410 Terry Ave. N Seattle, WA 98109	NINJIO Hosted Platform for Training & Phishing. PII: Full Name, Email Address, Department, Phone Number, Manager, Title, Location, (additional attributes chosen by Customer), data generated related to the performance of individuals participating in the program: training results, phishing campaign results. IP Address, Operating System, Browser, Device Type.
Kaseya Holdings Inc. - Datto	877-811-0577	101 Merritt 7 , 7th floor Norwalk, CT 06851	Ninjio Operational Systems backup - Microsoft 365 backup.
Twilio Inc.	415-390-2337	375 Beale St #300 San Francisco, CA 94105	SMS relay related to 2FA and SMS Phishing. Processes phone number and employee ID.
Twilio Inc. - Sendgrid	303-552-0653	1801 California St, Suite 500 Boulder, CO 80202	SMTP relay for phishing and training: processes email and employee ID.
SolarWinds Corp - Loggly	415-969-5178	535 Mission St, Suite 2100 San Francisco, CA 94105	logging and monitoring of platform health and admin interactions
Intuit Inc. - Quickbooks	800-446-8848	2700 Coast Ave Mountain View, CA	financial data, billing PII
OneHub Inc	424-644-7774	1109 First Ave, Suite 406 Seattle, WA 98101	Content management system for Customer access to download content related to program deliverables. PII: Email Address & Name, access logs.
AirCall.io Inc.	888-240-6923	233 Park Ave S New York, NY 10003	inbound and outbound calling
Rustici Software, LLC (SCORM Cloud)	+1 866 497 2676	210 Gothic Court, Suite 300 Franklin, TN 37067, USA	SCORM hosting, launch, distribution, and learner activity tracking; may process user identifiers, email address, course assignment, completion, score, and launch/activity metadata.

Name	Phone	Address	Services/Sub-Processing Activities
Datadog, Inc.	+1 866 329 4466	620 8th Avenue, Floor 45 New York, NY 10018, USA	Application and infrastructure monitoring, security telemetry, alerting, and log analysis; may process IP/device data, administrator activity, technical identifiers, and limited Personal Data included in configured logs.
Stripe, LLC	privacy@stripe.com	354 Oyster Point Boulevard South San Francisco, CA 94080, USA	Payment processing, billing, and subscription administration; may process customer business-contact, billing, payment-method, transaction, fraud-prevention, and device data. Stripe may act as an independent controller for certain regulated payment activities.
Snowflake Inc.	privacy@snowflake.com	135 Constitution Drive Menlo Park, CA 94025, USA	Cloud data warehousing and analytics; may process account/profile identifiers, customer-configured attributes, training and phishing-simulation outcomes, reporting metrics, and operational metadata.
Sigma Computing, Inc. (Sigma BI Reporting)	privacy@sigmacomputing.com	116 New Montgomery Street, Suite 700 San Francisco, CA 94105, USA	Business-intelligence reporting and visualization through governed access to Snowflake; may access or query authorized user, training, phishing-simulation, risk, and program-reporting data.
Oracle America, Inc. (Oracle NetSuite)	+1 737 867 1000	2300 Oracle Way Austin, TX 78741, USA	Enterprise resource planning, contracting, invoicing, and billing administration; may process customer business-contact, account, order, invoice, payment-status, and transaction records.
Mailgun Technologies, Inc. (a Sinch company)	dpo@sinch.com	112 E. Pecan Street, #1135 San Antonio, TX 78205, USA	Transactional email delivery and related deliverability services; may process recipient email address, user/employee identifier, message metadata and content, IP address, delivery events, and suppression/opt-out data.

Appendix 3
UK International Data Transfer Addendum
to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date:	As of the Effective Date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who received the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Ninjio, LLC Trading name (if different); N/A Main address (if a company registered address): 880 Hampshire Road, Suite B, Westlake Village, CA 91361 Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): N/A Job Title: Contact details including email: UK GDPR Representative: Name: Address: Email:	Full Name (optional): Laura Bell Main Job Title: CTO Contact details including email: 880 Hampshire Road, Suite B, Westlake Village, CA 91361 Email: lmain@ninjio.com and compliance@ninjio.com
Signature (if required for the purposes of Section 2)	See signature page attached to the DPA.	See signature page attached to the DPA.

Table 2: Selected SCCs, Modules, and Selected Clauses

Addendum EU SCCs	[_] The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: _____ Reference (if any): _____ Other identifier (if any): _____ Or [X] the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorization or General Authorization)	Clause 9a (Time Period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No	N/A	N/A	–	–	–
2	Yes	Yes	No	General Authorization	30 Days	–
3	Yes	Yes	No	General Authorization	30 Days	–
4	No	N/A	N/A	–	–	N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex IA of Appendix 2 (EU SCCs)
Annex 1B: Description of Transfer: See Annex IB of Appendix 2 (EU SCCs)
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: See Annex II of Appendix 2 (EU SCCs)
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex III of Appendix 2 (EU SCCs)

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: [_] Importer [X] Exporter [_] neither Party

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the 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 18 of those Mandatory Clauses.