Data Processing Addendum

Niural Data Processing Addendum : Version [_____] 2026

Between

Niural Inc.

a Delaware registered company, having its registered address at
16192 Coastal Hwy, Lewes, DE 19958
and its affiliates
(hereinafter "Niural")

And

Client Name: .....

Client Address: .....

(hereinafter "Client")

(individually, a "Party" and collectively, the "Parties")

Table of Contents

Table of Contents 2
1. Definitions 4
2. Scope and Roles 5
2.1 Roles of the Parties 5
2.2 Processing by Niural as an Independent Controller 5
2.3 Compliance 5
2.4 Term 5
3. Processing Instructions 6
4. Niural Obligations as Processor 6
5. Client Obligations 7
6. Data-Subject Requests and Regulatory Assistance 7
7. Subprocessors 8
7.1 General Authorization 8
7.2 Third Parties That Are Not Subprocessors 8
7.3 Client-Selected Third Parties and Integrations 8
7.4 Subprocessor List 9
7.5 Notice of Changes 9
7.6 Objection 9
7.7 Termination for Unresolved Objection 9
7.8 Responsibility 9
8. Security and Incidents 9
9. Return and Deletion 10
10. International Transfers 10
10.1 Restricted Transfers 10
10.2 EU SCCs — Module Selection 11
10.3 Completion of the EU SCCs 11
10.4 United Kingdom 11
10.5 Switzerland 11
10.6 Conflict and Invalidation 12
11. Audits and Compliance Information 12
12. Liability and Precedence 13
13. Schedules 13
Signatories 13
Schedule 1 — Details of Processing 15
A. Subject matter, nature and purpose of the Processing 15
B. Duration of the Processing 15
C. Frequency of the Processing 15
D. Categories of Data Subjects 15
E. Categories of Customer Personal Data 15
F. Special Categories of Personal Data 16
G. Processing Operations 16
Schedule 2 — Technical and Organizational Measures 17
Schedule 3 — Contact Details of the Parties 19

Parties entitled to issue instructions and recipients of instructions 19
Privacy contacts 19
Schedule 4 — Standard Contractual Clauses, Annex I 20
A. List of Parties 20
B. Description of Transfer 20
C. Competent Supervisory Authority 21
Schedule 5 — Subprocessors 22
Schedule 6 — Artificial Intelligence 23

1. Definitions

1.1 This Data Processing Addendum ("DPA" or "Addendum"), including its Schedules, forms part of the Niural Terms of Service found at https://www.niural.com/terms-of-service, unless Client has entered into a superseding written subscription agreement with Niural, in which case it forms part of that written agreement (in either case, the "Agreement").

1.2 Capitalized terms used in this DPA and not otherwise defined have the meaning given to them under the applicable Data Protection Laws or, if not defined thereunder, under the EU GDPR. In relation to the CCPA and other applicable U.S. State Privacy Laws, terms used in provisions of this DPA where such laws apply shall be read as follows: "Personal Data" means "Personal Information"; "Controller" means "Business"; "Processor" means "Service Provider" or "Contractor"; and "Data Subject" means "Consumer".

1.3 In this DPA:

"Customer Personal Data" means Personal Data that Client or its authorized users submit to, make available to, or cause Niural to collect or receive in connection with the Services, to the extent Niural processes that Personal Data on behalf of Client. Customer Personal Data excludes Personal Data Niural processes as an independent Controller.

"Data Protection Laws" means all data protection and privacy laws and regulations applicable to a Party's Processing of Personal Data under the Agreement, including, where applicable, EU/UK Data Protection Laws, Non-EU Data Protection Laws, and any other applicable data protection laws.

"EU/UK Data Protection Laws" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "EU GDPR"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to, or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

"Europe" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

"Non-EU Data Protection Laws" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"); other applicable U.S. state privacy laws ("U.S. State Privacy Laws"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018, and its implementing regulations.

"Restricted Transfer" means: (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area or Switzerland to a country outside of the European Economic Area or Switzerland which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Niural or its Subprocessors. A Security Incident does not include unsuccessful attempts or activities

that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial-of-service attacks, and other network attacks on firewalls or networked systems.

"Services" means the payroll, human resources, workforce management, employment, contractor, benefits, payment, and related products and services provided by Niural under the Agreement.

"Standard Contractual Clauses" or "SCCs" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 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 (the "EU SCCs"); and (ii) where the UK GDPR applies, the EU SCCs as amended by the UK Addendum. The Standard Contractual Clauses are incorporated by reference and form an integral part of this DPA.

"Subprocessor" means any third party engaged by Niural (including any Niural affiliate) that Processes Customer Personal Data on Niural's behalf in connection with the Services.

"Swiss DPA" means the Swiss Federal Act on Data Protection of 25 September 2020, as amended or superseded from time to time, and its implementing ordinances.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner under s.119A(1) of the Data Protection Act 2018, as amended or superseded from time to time.

2. Scope and Roles

2.1 Roles of the Parties

With respect to Customer Personal Data processed by Niural on behalf of Client in connection with the Services, Client acts as a Controller or Processor, as applicable, and Niural acts as a Processor or Subprocessor.

2.2 Processing by Niural as an Independent Controller

This DPA does not apply to personal information Niural processes as an independent Controller for its own purposes, including in connection with account administration, security, fraud prevention, legal and regulatory compliance, billing, tax, PEO, EOR, AOR, benefits, employment, or other purposes described in the Agreement or Niural's Privacy Policy.

Where Niural Processes Personal Data as an independent Controller, Niural is solely responsible for complying with the obligations applicable to a Controller under Data Protection Laws in respect of that Processing, and Client is solely responsible for complying with the obligations applicable to it in respect of Personal Data it Processes as a Controller.

2.3 Compliance

Each Party shall comply with the obligations applicable to it under the Data Protection Laws with respect to the Processing of Personal Data covered by this DPA.

2.4 Term

2.4.1 The term of this DPA is coextensive with the term of the Agreement. Termination or expiry of the Agreement shall also terminate this DPA, save for those provisions that by their nature survive.

2.4.2 Either Party may terminate this DPA on written notice in the event of the other Party's serious breach of statutory or contractual data protection provisions under the Data Protection Laws, insofar as the terminating Party cannot reasonably be expected to continue this DPA.

2.4.3 Termination of this DPA at any time and for any reason does not exempt either Party from its obligations under the Data Protection Laws relating to the collection, Processing and use of Personal Data.

3. Processing Instructions

3.1 Niural shall Process Customer Personal Data only on documented instructions from Client, including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by Union, Member State, or other applicable law to which Niural is subject. The Agreement, this DPA, and Client's and its authorized users' configuration and use of the Services constitute Client's complete and final documented instructions to Niural for the Processing of Customer Personal Data. Additional or alternate instructions must be agreed in writing between the Parties.

3.2 Niural shall inform Client if, in Niural's reasonable opinion, an instruction infringes applicable Data Protection Laws, unless Niural is prohibited from doing so by law. Niural may suspend performance of the affected instruction until it is confirmed, withdrawn, or modified.

3.3 Where Niural is required by applicable law to Process Customer Personal Data other than on Client's instructions, Niural shall inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.4 To the extent the CCPA or other U.S. State Privacy Laws apply, Niural acts as a Service Provider (or Contractor, as applicable) with respect to Customer Personal Data. Niural shall not: (a) sell or share Customer Personal Data; (b) retain, use, or disclose Customer Personal Data for any purpose other than the business purposes specified in the Agreement, including for a commercial purpose other than the provision of the Services; (c) retain, use, or disclose Customer Personal Data outside the direct business relationship between the Parties; or (d) combine Customer Personal Data with personal information received from or on behalf of another person, or collected from its own interaction with a consumer, except as permitted under applicable law. Niural certifies that it understands and will comply with these restrictions.

4. Niural Obligations as Processor

With respect to Customer Personal Data, Niural shall:

- process Customer Personal Data only on Client's documented instructions in accordance with Section 3;
- ensure that persons authorized to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and receive appropriate data protection training;
- implement and maintain appropriate technical and organizational measures to protect Customer Personal Data in accordance with Section 8 and Schedule 2;
- engage Subprocessors only in accordance with Section 7;
- taking into account the nature of the Processing, assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to requests for exercising Data Subject rights, in accordance with Section 6;

- provide reasonable assistance to Client with data protection impact assessments and prior consultations with supervisory authorities, in each case solely in relation to the Processing of Customer Personal Data and taking into account the nature of the Processing and the information available to Niural;
- notify Client of a Security Incident without undue delay after becoming aware of it, in accordance with Section 8;
- at Client's election, delete or return Customer Personal Data on termination or expiry of the Services, subject to any legal or regulatory retention requirement, in accordance with Section 9;
- make available to Client information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and Article 28 of the EU GDPR, and allow for and contribute to audits in accordance with Section 11;
- inform Client if an instruction appears to Niural to be unlawful, in accordance with Section 3.2; and
- maintain a record of Processing activities carried out on behalf of Client as required by Article 30(2) of the EU GDPR.

5. Client Obligations

5.1 Client shall provide Niural with all information reasonably necessary for Niural to perform the Services.

5.2 Client represents and warrants that: (a) it has established and will maintain a valid legal basis for the Processing of Customer Personal Data under this DPA; (b) it has provided all notices and obtained all consents, permissions, and rights necessary under Data Protection Laws for Niural and its Subprocessors to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement; and (c) its instructions to Niural comply with applicable Data Protection Laws.

5.3 Client is responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which it acquired that data, and for its own and its authorized users' configuration and use of the Services, including any decision to enable an integration or transmit Customer Personal Data to a third party selected by Client.

5.4 Where Client is itself a Processor acting on behalf of a third-party Controller, Client represents and warrants that it has obtained all necessary authorizations from that Controller, including authorization to appoint Niural as a Subprocessor, and that its instructions to Niural reflect the instructions of that Controller.

5.5 Client shall not submit to the Services any special categories of Personal Data, or Personal Data relating to children, other than as reasonably necessary for and contemplated by the Services as described in Schedule 1.

6. Data-Subject Requests and Regulatory Assistance

6.1 The Services provide Client with functionality that enables Client to retrieve, correct, delete, restrict, or export Customer Personal Data, and Client may use that functionality to assist it in responding to Data Subject requests.

6.2 If Niural receives a request from a Data Subject in relation to Customer Personal Data, Niural shall promptly inform Client and shall advise the Data Subject to submit the request to Client. Niural shall not respond to the request itself except as legally required or as instructed by Client.

6.3 Taking into account the nature of the Processing, Niural shall provide Client with reasonable assistance, insofar as possible, to enable Client to respond to Data Subject requests that Client is not able to address through the functionality of the Services.

6.4 Niural shall, taking into account the nature of the Processing and the information available to Niural, provide reasonable assistance to Client with data protection impact assessments and prior consultations with supervisory authorities, in each case where required by applicable Data Protection Laws and solely in relation to Processing of Customer Personal Data.

6.5 If Niural receives a legally binding request from a public authority for disclosure of Customer Personal Data, Niural shall, unless prohibited by law, notify Client, use reasonable efforts to redirect the authority to request the data directly from Client, and, where appropriate and legally permitted, challenge a request that Niural reasonably believes is unlawful or overbroad.

7. Subprocessors

7.1 General Authorization

Client generally authorizes Niural to engage Subprocessors in connection with the Services. Niural will enter into a written agreement with each Subprocessor imposing data-protection obligations appropriate to the nature of the processing and no less protective in material respects than those imposed on Niural under this DPA. Niural remains responsible for its Subprocessors to the extent required by applicable law and the Agreement.

7.2 Third Parties That Are Not Subprocessors

Certain third parties, including regulated financial institutions, payment service providers, insurers, professional advisers, and government authorities, may process Personal Data as independent Controllers where they determine their own purposes and means of Processing or process Personal Data to comply with their own legal or regulatory obligations. Such parties are not Subprocessors under this DPA to the extent of that independent-controller Processing.

7.3 Client-Selected Third Parties and Integrations

Where Client independently selects a third party, or instructs or configures the Services to transmit Personal Data to a third party that Niural has not engaged to deliver the Services, including through an integration, connector, application programming interface, or file transfer enabled or authorized by Client, that third party is not a Subprocessor. Client is responsible for its selection of, and its relationship and contractual arrangements with, that third party, and for ensuring an appropriate legal basis and, where applicable, an appropriate transfer mechanism for the disclosure. This Section 7.3 does not apply to a third party that Niural selects and engages to Process Customer Personal Data on Niural's behalf in order to deliver the Services; such a third party is a Subprocessor and Sections 7.1 and 7.4 to 7.8 apply to it.

7.4 Subprocessor List

Niural maintains a current list of Subprocessors engaged in connection with the Services at https://www.niural.com/subprocessors or a successor location notified to Client. The list identifies each Subprocessor, its processing location, and the nature of the Processing it performs.

7.5 Notice of Changes

Niural shall provide Client with written notice of any intended addition or replacement of a Subprocessor at least fifteen (15) days before Niural authorizes that Subprocessor to Process Customer Personal Data.

Notice may be provided by updating the subprocessor list and sending notice to Client's contact under the Agreement or another contact designated by Client.

Where a change is required urgently to protect the security or continuity of the Services, or to comply with applicable law, Niural may engage the Subprocessor on shorter notice and shall notify Client as soon as reasonably practicable.

7.6 Objection

Client may object to the appointment of a new Subprocessor on reasonable data-protection grounds by giving written notice to Niural within fifteen (15) days after receiving Niural's notice. The Parties shall discuss the objection in good faith and Niural shall use reasonable efforts to make available to Client a change in configuration or an alternative arrangement that avoids the Processing of Customer Personal Data by the objected-to Subprocessor.

7.7 Termination for Unresolved Objection

If Niural is unable to make a reasonable alternative available within a reasonable period, Client may, as its sole and exclusive remedy, terminate the specific Service that cannot be provided without the objected-to Subprocessor, by written notice to Niural. Termination under this Section 7.7 does not entitle Client to terminate any other part of the Services or the Agreement, and Client remains liable for fees accrued prior to the effective date of termination.

7.8 Responsibility

Niural shall be liable for the acts and omissions of its Subprocessors in the Processing of Customer Personal Data to the same extent Niural would be liable if performing the services of the Subprocessor directly under this DPA, subject to the limitations of liability in the Agreement.

8. Security and Incidents

8.1 Niural shall implement and maintain technical and organizational measures appropriate to the risk to ensure the security, confidentiality, integrity, and availability of Customer Personal Data it Processes, as described in Schedule 2.

8.2 The measures described in Schedule 2 are subject to technical progress and development. Niural may update or modify those measures provided that the updated or modified measures do not result in a material degradation of the overall security of the Services.

8.3 Niural shall ensure that persons authorized to Process Customer Personal Data are subject to binding obligations of confidentiality and receive appropriate training on their responsibilities in relation to Personal Data.

8.4 Niural shall notify Client of a Security Incident without undue delay after becoming aware of it. The notification shall, to the extent known and permitted by law, describe the nature of the Security Incident, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address it. Niural shall provide further information as it becomes available and shall take reasonable steps to mitigate and remediate the Security Incident.

8.5 Niural's notification of or response to a Security Incident under this Section 8 is not an acknowledgement by Niural of any fault or liability with respect to the Security Incident.

8.6 Client is responsible for determining whether a Security Incident requires notification to a supervisory authority or to affected Data Subjects and for making any such notification, except where Niural is required to make a notification in its own capacity under applicable law.

9. Return and Deletion

9.1 On termination or expiry of the Services, Niural shall, at Client's election, delete or return Customer Personal Data to Client. Client may request the return or export of Customer Personal Data through the functionality of the Services during the term and for any period made available through the Services or otherwise agreed by the Parties.

9.2 Following expiry of the export period described in Section 9.1, Niural shall delete Customer Personal Data in accordance with its data retention practices, except to the extent Niural is required to retain Customer Personal Data by applicable law, including payroll, tax, employment, benefits, anti-money-laundering, sanctions, and financial recordkeeping requirements, or where retention is necessary for the establishment, exercise, or defence of legal claims.

9.3 Customer Personal Data retained under Section 9.2 shall remain subject to the confidentiality and security obligations of this DPA for so long as it is retained, and shall not be Processed for any purpose other than the purpose for which it is retained.

9.4 Customer Personal Data contained in backups or archives shall be deleted in accordance with Niural's ordinary backup rotation and retention cycle.

10. International Transfers

10.1 Restricted Transfers

Where a transfer of Personal Data under this DPA is a Restricted Transfer, that transfer shall be subject to the applicable Standard Contractual Clauses, which are incorporated into this DPA by reference, unless an alternative transfer mechanism recognised under applicable Data Protection Laws (including an adequacy decision or approved certification framework) applies to the transfer, in which case that mechanism shall apply for so long as it is valid and available.

10.2 EU SCCs — Module Selection

The module of the EU SCCs applicable to a transfer shall be determined by the roles of the Parties in respect of that transfer, as follows:

- Module Two (Controller to Processor) applies where Client is a Controller and Niural is a Processor.
- Module Three (Processor to Processor) applies where Client is a Processor and Niural is a Subprocessor.
- Module One (Controller to Controller) applies only where both Parties are independent Controllers for the relevant transfer.

Where more than one module could apply to a transfer, the module corresponding to the Parties' actual roles for that Processing activity shall apply, and the EU SCCs shall be read accordingly.

10.3 Completion of the EU SCCs

In relation to Personal Data protected by the EU GDPR, the EU SCCs shall apply completed as follows:

- in Clause 7, the optional docking clause applies;
- in Clause 9 of Modules Two and Three, Option 2 (general written authorisation) applies, and the specified time period shall be fifteen (15) days, as set out in Section 7.5 of this DPA;
- in Clause 11, the optional redress language does not apply;

- in Clause 17, Option 1 applies, and the EU SCCs shall be governed by the law of Ireland;
- in Clause 18(b), disputes shall be resolved before the courts of Ireland;
- Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 4 to this DPA;
- Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA; and
- Annex III of the EU SCCs (where applicable) shall be deemed completed with the information set out in Schedule 5 to this DPA.

10.4 United Kingdom

For transfers subject to the UK GDPR, the UK International Data Transfer Addendum applies to the applicable EU SCC module. The UK Addendum shall be deemed executed between the Parties, and the EU SCCs, completed as set out in Sections 10.2 and 10.3, shall be deemed amended as specified by the UK Addendum in respect of such transfers. For the purposes of Table 4 of the UK Addendum, neither Party may end the UK Addendum as set out in Section 19 of the UK Addendum, save as permitted by that Section. The competent supervisory authority shall be the United Kingdom Information Commissioner's Office.

10.5 Switzerland

In relation to Personal Data protected by the Swiss DPA, the EU SCCs shall apply completed as set out in Sections 10.2 and 10.3, with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA; (iii) references to "EU", "Union" and "Member State law" shall be replaced with "Switzerland"; (iv) Clause 13(a) and Part C of Annex II shall be deleted; (v) references to the "competent supervisory authority" and "competent courts" shall be replaced with "the Swiss Federal Data Protection and Information Commissioner" and "the relevant courts in Switzerland"; (vi) Clause 17 shall be replaced to state that the Clauses are governed by the laws of Switzerland; and (vii) Clause 18 shall be replaced to state that any dispute arising from the Clauses shall be resolved by the applicable courts of Switzerland, and the Parties agree to submit to the jurisdiction of those courts.

10.6 Conflict and Invalidation

10.6.1 If any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

10.6.2 If the Standard Contractual Clauses or any other transfer mechanism relied on under this Section 10 is invalidated or restricted by a competent governmental entity or court, the Parties shall work together in good faith and without undue delay to implement an alternative or modified transfer mechanism that complies with applicable Data Protection Laws.

11. Audits and Compliance Information

11.1 Niural shall make available to Client information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and, where applicable, Article 28 of the EU GDPR.

11.2 Client agrees to exercise its audit rights under this DPA and the Standard Contractual Clauses in the first instance by requesting the then-current third-party audit reports, certifications, security documentation, or completed security questionnaires that Niural maintains in relation to the Services.

Where those materials do not reasonably enable Client to verify Niural's compliance, Sections 11.3 and 11.4 apply.

11.3 Client may, no more than once in any twelve (12) month period and on at least thirty (30) days' prior written notice, conduct an audit of Niural's Processing of Customer Personal Data. Any such audit shall: (a) be conducted during Niural's normal business hours; (b) be limited in scope to information and systems relevant to the Processing of Customer Personal Data; (c) not unreasonably interfere with Niural's business activities; (d) be subject to the confidentiality obligations of the Agreement; (e) not include access to the personal data, systems, or confidential information of any other Niural customer; and (f) be at Client's expense, save where the audit reveals a material breach by Niural of this DPA.

11.4 Client may conduct an audit more frequently than provided in Section 11.3 where required by a supervisory authority with jurisdiction over Client, or following a Security Incident affecting Customer Personal Data.

11.5 Where an auditor is appointed by Client, that auditor shall not be a competitor of Niural and shall execute a confidentiality agreement reasonably acceptable to Niural before commencing the audit.

11.6 The Parties agree that the audit rights set out in this Section 11 satisfy the audit requirements of Clause 8.9 of the EU SCCs (Modules Two and Three).

12. Liability and Precedence

12.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement, except to the extent such exclusions and limitations are not permitted by applicable Data Protection Laws.

12.2 In the event of a conflict, the following order of precedence applies: (a) the Standard Contractual Clauses; (b) this DPA; and (c) the remainder of the Agreement.

12.3 This DPA and its Schedules constitute the entire agreement between the Parties in relation to the Processing of Customer Personal Data and replace all previous agreements between the Parties relating to that subject matter.

12.4 If any provision of this DPA is or becomes invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the Parties shall replace the invalid provision with a valid provision that comes closest to its purpose and economic effect.

12.5 Amendments and additions to this DPA must be made in writing and signed by both Parties. This requirement also applies to any amendment of this written-form requirement. For the avoidance of doubt, updates to the subprocessor list made in accordance with Section 7, and updates to Schedule 2 made in accordance with Section 8.2 that do not materially reduce the overall security of the Services, do not constitute an amendment to this DPA and may be made by Niural without a signed writing.

12.6 Except as otherwise required by the Standard Contractual Clauses or applicable Data Protection Laws, this DPA is governed by, and disputes arising under it are subject to, the governing law and jurisdiction specified in the Agreement. For the avoidance of doubt, the EU SCCs are governed by the law of Ireland and disputes arising under them shall be resolved before the courts of Ireland in accordance with Section 10.3; the UK Addendum and any other mandatory transfer instrument are governed as required by that instrument.

13. Schedules

The following Schedules form an integral part of this DPA:

- Schedule 1 — Details of Processing
- Schedule 2 — Technical and Organizational Measures (EU SCCs Annex II)
- Schedule 3 — Contact Details of the Parties
- Schedule 4 — Standard Contractual Clauses, Annex I
- Schedule 5 — Subprocessors (EU SCCs Annex III)
- Schedule 6 — Artificial Intelligence

Signatories

On behalf of Client:

Client Full Legal Name: ……

Signatory Name: ……

Position: ……

Date, Signature: ……

On behalf of Niural:

Full Legal Name: Niural Inc. ……

Signatory Name: ……

Position: ……

Date, Signature: ……

Schedule 1 — Details of Processing

A. Subject matter, nature and purpose of the Processing

Niural Processes Customer Personal Data as necessary to provide, maintain, secure, support, and update the Services under the Agreement, including the provision of payroll, human resources, workforce management, employment, contractor, benefits, and payment products and services, and to provide technical support to Client.

B. Duration of the Processing

For the term of the Agreement, plus the period following termination or expiry described in Section 9 of this DPA and any period for which retention is required by applicable law.

C. Frequency of the Processing

Continuous for the duration of the Services.

D. Categories of Data Subjects

Customer Personal Data may relate to the following categories of Data Subjects. This list is indicative and not exhaustive; the actual categories are determined by Client's configuration and use of the Services.

- prospective, current, and former employees of Client and its affiliates;
- contractors, consultants, and other workers engaged by Client and its affiliates;
- dependents, beneficiaries, and emergency contacts of the foregoing;
- Client administrators and authorized users of the Services;
- candidates and applicants; and
- vendors, brokers, accountants, advisers, and other third parties whose information Client submits to the Services.

E. Categories of Customer Personal Data

Customer Personal Data may include the following categories. This list is indicative and not exhaustive; the actual categories are determined by Client's configuration and use of the Services.

- contact and identity information, including name, postal address, email address, telephone number, and date of birth;
- payroll, compensation, bonus, commission, equity, expense, and timekeeping data;
- tax information and government identifiers, including taxpayer identification and social security or national insurance numbers;
- bank account, payment, and remittance details;
- employment, onboarding, job, performance, leave, and termination data;
- benefits elections, eligibility, dependent and beneficiary information, and qualifying life events;
- immigration and work-authorization information;
- identity verification data, including copies of government-issued identification and, where the identity verification workflow is used, a photograph submitted by the individual;
- device, usage, log, support, and integration data generated in connection with use of the Services; and
- other information configured or submitted by Client or its authorized users.

F. Special Categories of Personal Data

To the extent Client's configuration and use of the Services requires it, Customer Personal Data may include the following special categories of Personal Data or data otherwise treated as sensitive under applicable Data Protection Laws:

- biometric data, where the identity verification workflow processes a photograph against a government-issued identification document for the purpose of uniquely identifying an individual;
- government identification numbers, as may be present on a copy of a government-issued identification document;
- health, disability, and medical information, to the extent submitted in connection with benefits administration, leave, accommodation, or occupational health requirements;
- financial account information; and
- other special categories submitted by Client where required for statutory reporting or benefits purposes.

Personal Data, including special categories of Personal Data, is protected in accordance with Section 8 and Schedule 2.

G. Processing Operations

- collection, recording, organization, structuring, storage, retrieval, use, and erasure as necessary to provide, maintain, secure, and update the Services;
- transmission and disclosure to Subprocessors and to recipients designated or authorized by Client in connection with the Services;
- provision of technical and customer support to Client; and
- disclosures in accordance with the Agreement or as compelled by applicable law.

Schedule 2 — Technical and Organizational Measures

(EU SCCs Annex II)

Niural implements and maintains technical and organizational measures designed to ensure a level of security appropriate to the risk presented by the Processing of Customer Personal Data, addressing at minimum the control domains set out below.

Control domain	Measures
Access control and least privilege	Niural maintains access control policies and grants access to systems and Customer Personal Data on a role-based, least-privilege and need-to-know basis. Access is provisioned on approval and removed following role change or termination, and access rights are subject to review.
Authentication	Access to systems that store or Process Customer Personal Data requires authentication. Niural applies password complexity requirements and, where appropriate to the relevant system and level of access, multi-factor authentication, including for administrative and remote access.
Encryption	Niural uses encryption in transit and, where appropriate to the relevant system and data, encryption at rest, together with controlled access to encryption keys.
Logging and monitoring	Security-relevant events, including authentication and administrative activity, are logged. Logs are retained for a defined period, are protected against unauthorized modification, and are monitored for anomalous activity.
Incident response	Niural maintains an incident response process defining roles and responsibilities, severity classification, escalation, containment and remediation, customer notification, and post-incident review.
Business continuity and backups	Niural maintains business continuity and disaster recovery arrangements appropriate to the Services, and performs backups of production data with defined retention and restricted access. Restoration procedures are tested at intervals appropriate to the risk.
Personnel confidentiality and training	Personnel with access to Customer Personal Data are subject to written confidentiality obligations that survive termination of engagement, and receive security and data protection training appropriate to their role. Background screening is performed where permitted by applicable law.
Vendor and Subprocessor risk management	Subprocessors are assessed before engagement against security and data protection criteria appropriate to the nature of the Processing, are subject to written data protection terms in accordance with Section 7 of the DPA, and are subject to review during the engagement.
Vulnerability and change management	Niural maintains a change management process covering testing, review, and approval of changes to production systems, together with processes designed to identify and remediate vulnerabilities, with remediation prioritized by severity.
Data segregation and deletion	Customer Personal Data is logically segregated so that data relating to different customers and different purposes is Processed separately.

Control domain	Measures
	Niural maintains processes for the deletion and secure disposal of Customer Personal Data in accordance with Section 9 of the DPA.

These measures are subject to technical progress and development. Niural may update or modify them in accordance with Section 8.2 of this DPA, provided that no update or modification results in a material degradation of the overall security of the Services.

Schedule 3 — Contact Details of the Parties

Parties entitled to issue instructions and recipients of instructions

Niural

Name	Address / Telephone	Email
Niural Legal	16192 Coastal Hwy, Lewes, DE 19958	legal@niural.com

Client

Name	Address / Telephone	Email

Privacy contacts

Niural Privacy Contact

Name	Address / Telephone	Email
Niural Privacy Contact	16192 Coastal Hwy, Lewes, DE 19958	legal@niural.com

Client Privacy Contact / Data Protection Officer (if applicable)

Name	Address / Telephone	Email

Schedule 4 — Standard Contractual Clauses, Annex I

A. List of Parties

Data exporter

Name:	As detailed in the Client details on page 1.
Address:	As detailed in the Client details on page 1.
Contact person's name, position and contact details:	As detailed in Schedule 3.
Activities relevant to the data transferred under these Clauses:	Receipt of the Services under the Agreement, and submission of Customer Personal Data to Niural for Processing in connection with the Services.
Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.

Role (controller/processor):	Controller or Processor, as determined under Section 2 of the DPA for the relevant Processing activity.

Data importer

Name:	Niural Inc.
Address:	16192 Coastal Hwy, Lewes, DE 19958, United States
Contact person's name, position and contact details:	As detailed in Schedule 3.
Activities relevant to the data transferred under these Clauses:	Processing of Customer Personal Data necessary to provide the Services pursuant to the terms of the Agreement.
Signature and date:	This Annex I shall be deemed executed upon execution of the DPA.
Role (controller/processor):	Processor or Subprocessor, as determined under Section 2 of the DPA for the relevant Processing activity.

B. Description of Transfer

Categories of data subjects whose personal data is transferred:	As detailed in Schedule 1, Section D.
Categories of personal data transferred:	As detailed in Schedule 1, Section E.
Sensitive data transferred (if applicable) and applied restrictions or safeguards:	As detailed in Schedule 1, Section F. Personal Data, including sensitive Personal Data, is protected in accordance with Section 8 of the DPA and Schedule 2.
The frequency of the transfer:	Continuous for the duration of the Services.
Nature of the processing:	As detailed in Schedule 1, Sections A and G.
Purpose(s) of the data transfer and further processing:	As detailed in Schedule 1, Section A.
The period for which the personal data will be retained:	As detailed in Schedule 1, Section B and Section 9 of the DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	The subject matter, nature, purpose, and duration of processing by Subprocessors are limited to the activities necessary to support Niural's provision of the Services, and continue for the period during which the relevant Subprocessor provides services to Niural. The Subprocessors engaged in connection with the Services are identified through the list incorporated by reference in Schedule 5.

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 SCCs):	Where the EU GDPR applies, the competent supervisory authority shall be determined in accordance with Clause 13 of the Standard Contractual Clauses. Where the UK GDPR applies, the competent supervisory authority shall be the United Kingdom Information Commissioner's Office. Where the Swiss DPA applies, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

Schedule 5 — Subprocessors

(EU SCCs Annex III)

The current list of Niural's authorized Subprocessors, including processing location and function, is available at https://www.niural.com/subprocessors and is incorporated into this DPA by reference. Niural may add or replace Subprocessors in accordance with Section 7.

Third parties that Process Personal Data as independent Controllers, to the extent of that independent-controller Processing, are not Subprocessors and are not included in that list; see Section 7.2. Third parties selected by Client, including Client-enabled integrations, are addressed under Section 7.3.

Schedule 6 — Artificial Intelligence

This Schedule forms part of the DPA. Capitalized terms not defined herein have the meanings given in the DPA.

1. Niural may use artificial intelligence and automated processing technologies ("AI Technologies") in connection with the Services. Niural may update or replace such technologies at its discretion, provided that the data protection obligations in the DPA continue to apply. Niural shall notify Client of any material change to the AI Technologies that significantly alters how Customer Personal Data is Processed, such as the introduction of a new third-party AI service provider, in accordance with the notification procedures in Section 7 of the DPA.

2. Where a third-party provider of AI Technologies Processes Customer Personal Data on Niural's behalf in connection with the Services, that provider is a Subprocessor for the purposes of this DPA and is subject to Section 7, including the requirement of a written agreement imposing data-protection obligations no less protective in material respects than those imposed on Niural, and the subprocessor list, notice, and objection provisions of that Section.

3. Niural shall not use Customer Personal Data to train general-purpose artificial intelligence or machine learning models. This restriction does not limit Niural from:

- using Customer Personal Data as necessary to deliver, operate, and improve the Services for Client; or
- using data that has been aggregated or de-identified such that it cannot reasonably be used to identify any individual, in accordance with applicable Data Protection Laws, for product analytics and service improvement.

4. Niural shall ensure that third-party providers of AI Technologies do not use Customer Personal Data to train general-purpose artificial intelligence or machine learning models. Niural shall contract with each

such provider on terms that prohibit that use, and shall not submit Customer Personal Data to any AI Technology that does not operate under such terms.

5. Niural shall maintain appropriate technical and organizational measures for AI Technologies consistent with Schedule 2 of the DPA, including access controls, logging of automated processing operations, and safeguards against unauthorized use of Customer Personal Data for model training.

6. The Parties shall cooperate in good faith regarding any regulatory requirements applicable to AI Technologies used in connection with the Services, including the EU AI Act (Regulation (EU) 2024/1689) as it becomes applicable. Obligations under such requirements shall be allocated between the Parties in accordance with their respective roles under applicable law.