OriginsNext Data Processing Addendum

Effective starting: 15 July 2026

This Data Processing Addendum (**DPA**) supplements the OriginsNext Client Terms, Engagement Letter or other agreements in place between OriginsNext and a Client (the 'Agreement'). This DPA covers the use of OriginsNext's Platform and related Services by a Client, as defined in the Client Terms. Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 9 of this DPA.

1. Scope and Term

1.1 Roles of the Parties.

(a) **Client Personal Data**. OriginsNext will Process Client Personal Data as a Processor on behalf of the Controller (the Client) in accordance with Controller's instructions as outlined in Section 2.1 (Client Instructions).

(b) **OriginsNext Account Data**. OriginsNext will Process OriginsNext Account Data as a Controller for the following purposes:

(i) to provide and improve the Platform;

(ii) to manage the Controller's relationship (communicating with the Controller and Users in accordance with their account preferences, responding to the Controller's inquiries and providing technical support, etc.),

(iii) to facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery; and

(iv) to carry out core business functions such as accounting, billing, and filing taxes.

(c) **OriginsNext Usage Data**. OriginsNext will Process OriginsNext Usage Data as a Controller for the following purposes:

(i) to provide, optimise, secure, and maintain the Platform;

(ii) to optimise user experience; and

(iii) to inform OriginsNext's business strategy.

(d) **Description of the Processing**. Details regarding the Processing of Personal Data by OriginsNext are stated in Schedule 1 (Description of Processing).

1.2 **Term of the DPA.** The term of this DPA coincides with the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which OriginsNext ceases all Processing of Client Personal Data).

1.3 **Order of Precedence.** If there is any conflict or inconsistency among the following documents, the order of precedence is:

(a) the main body of this DPA;

(b) the applicable terms stated in Schedule 2 (Region-Specific Terms including any transfer provisions); and

(c) the Agreement.

2. Processing of Personal Data

2.1 **Client Instructions.** OriginsNext must Process Client Personal Data in accordance with the documented lawful instructions of the Controller as stated in the Agreement (including this DPA) and respective Engagement Letters, as necessary to:

(a) provide the Platform and related Services to the Client and enable the use of various features and functionalities in accordance with the Documentation (including as directed by Users through the Platform),

(b) investigate security incidents and enforce the End User Terms; or

(c) comply with its legal obligations. OriginsNext will notify the Controller if it becomes aware, or reasonably believes, that the Controller's instructions violate Applicable Data Protection Law.

2.2 **Confidentiality.** OriginsNext must treat Client Personal Data as the Controller's Confidential Information under the Agreement. OriginsNext must ensure personnel authorised to Process Personal Data are bound by written or statutory obligations of confidentiality.

2.3 **No Sale of Personal Data**. OriginsNext will not sell, rent, or otherwise commercialise Client Personal Data, and will Process Client Personal Data only for the purposes set out in this DPA and the Agreement.

3. Security

3.1 **Security Measures.** OriginsNext has implemented and will maintain appropriate technical and organisational measures designed to protect the security, confidentiality, integrity and availability of Client Personal Data and protect against Security Incidents. Client is responsible for configuring the Platform and using features and functionalities made available by OriginsNext to maintain appropriate security relevant to the nature of Client Data. Client acknowledges that the Security Measures are subject to technical progress and development and that OriginsNext may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Platform during a Subscription Term.

3.2 **Security Incidents.** OriginsNext must notify Client without undue delay after becoming aware of a Security Incident. OriginsNext must make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within OriginsNext's reasonable control. Upon Client's request and taking into account the nature of the Processing and the information available to OriginsNext, OriginsNext must assist Client by providing information reasonably necessary for Client to meet its Security Incident notification obligations under Applicable Data Protection Law. OriginsNext's notification of a Security Incident is not an acknowledgment by OriginsNext of its fault or liability.

4. Sub-processing

4.1 **General Authorisation.** By entering into this DPA, the Controller provides general authorisation for OriginsNext to engage Sub-processors to Process Client Personal Data. OriginsNext must:

(a) enter into a written agreement with each Sub-processor ensuring data protection terms are in place that require the Sub-processor to protect Client Personal Data to the standard required by Applicable Data Protection Law and to the same standard provided by this DPA; and

(b) remain liable to the Controller if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant Processing activities under the Agreement.

4.2 **Notice of New Sub-processors.** OriginsNext maintains an up-to-date list of its Sub-processors in Schedule 3. OriginsNext will update this list at least fourteen (14) days before allowing any new Sub-processor to Process Client Personal Data (the Sub-processor Notice Period). The Controller is responsible for regularly reviewing this list.

4.3 **Objection to New Sub-processors.** The Controller may object to OriginsNext's appointment of a new Sub-processor during the Sub-processor Notice Period. If the Controller objects, OriginsNext will work with the Controller to find a suitable solution, but if no solution can be reached, the Controller, as its sole and exclusive remedy, may terminate the applicable Engagement Letter or Agreement in accordance with the termination provisions outlined therein.

5. Assistance and Cooperation Obligations

5.1 **Data Subject Rights**. Taking into account the nature of the Processing, OriginsNext must provide reasonable and timely assistance to the Controller to enable the Controller to respond to requests for exercising a data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Client Personal Data.

5.2 **Cooperation Obligations**. Upon the Controller's reasonable request, and taking into account the nature of the Processing, OriginsNext will provide reasonable assistance to the Controller in fulfilling the Controller's obligations under Applicable Data Protection Law (including data protection impact assessments and consultations with regulatory authorities), provided that the Controller cannot reasonably fulfill such obligations independently with help of available Documentation. Where such assistance is deemed to be extraordinary or excessive, OriginsNext reserves the right to charge a reasonable fee for the provision of such assistance, subject to prior written agreement with the Controller.

5.3 **Third Party Requests**. Unless prohibited by Law, OriginsNext will promptly notify the Controller of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling OriginsNext to disclose Client Personal Data. In the event that OriginsNext receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Client Personal Data, OriginsNext will redirect such inquiries to the Controller, and will not provide any information unless required to do so under applicable Law.

5.4 **Further Obligations**. OriginsNext confirms that, in Processing Personal Data under this DPA, it: (a) Processes Personal Data on a valid legal basis under Applicable Data Protection Law; (b) will assist the Controller in meeting requests from data subjects; (c) maintains technical and administrative measures adequate to prevent Personal Data breaches and to ensure information security appropriate to its activities and the Processing; and (d) where it transfers Personal Data internationally, does so using mechanisms that are legally valid under Applicable Data Protection Law.

6. Deletion and Return of Client Personal Data

6.1 **During Subscription Term**. During the Subscription Term, Client and its Users may, through the available features of the Platform or by written instruction to OriginsNext, access, retrieve or delete Client Personal Data.

6.2 **Post Termination**. Following expiration or termination of the Agreement, OriginsNext will delete all Client Personal Data upon request from Client. Notwithstanding the foregoing, OriginsNext may retain Client Personal Data

(a) as required by Applicable Data Protection Law or

(b) in accordance with its standard backup or record retention policies, provided that, in either case, OriginsNext will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Client Personal Data and not further Process it except as required by Applicable Data Protection Law.

6.3 **Immutable and Permissioned Data**. The Controller acknowledges that, due to the immutable nature of the distributed ledger technology underlying the Platform, and in the case of Permissioned Data that has been shared with other Users or Participants, OriginsNext may be unable to amend or delete some

Client Personal Data. In such cases OriginsNext will continue to maintain the confidentiality of, and apply the protections of this DPA to, that data.

7. Audit

7.1 **Audit Reports**. OriginsNext undertakes periodic security and vulnerability audits by independent third-party auditors and/or internal auditors. Upon request, and on the condition that Client has entered into an applicable non-disclosure agreement with OriginsNext, OriginsNext will supply a summary copy of relevant audit report(s) (Report) to Client, so Client can verify OriginsNext's compliance with the audit standards against which it has been assessed, and this DPA. If Client cannot reasonably verify OriginsNext's compliance with the terms of this DPA, OriginsNext will provide written responses (on a confidential basis) to all reasonable requests for information made by Client related to its Processing of Client Personal Data, provided that such right may be exercised no more than once every twelve (12) months.

7.2 **On-site Audits**. Only to the extent Client cannot reasonably satisfy OriginsNext's compliance with this DPA through the exercise of its rights under Section 7.1 above, OriginsNext will, upon reasonable notice, provide Client with additional information or documentation as reasonably requested. On-site audits may only be conducted where mandated by a relevant regulatory authority and will be subject to mutual agreement on scope, timing, and confidentiality controls. Any such audit must be conducted at Client's expense, during OriginsNext's regular business hours, with at least sixty (60) calendar days' written notice, and occur no more than once every twelve (12) months.

8. International Provisions

8.1 To the extent OriginsNext Processes Personal Data protected by Applicable Data Protection Laws in one of the regions listed in Schedule 2 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Personal Data (directly or via onward transfer).

9. Definitions

Applicable Data Protection Law means all Laws applicable to the Processing of Personal Data under the Agreement.
OriginsNext Account Data means Personal Data relating to Client's relationship with OriginsNext, including:
(i) **Users** account information (e.g. name, email address);
(ii) billing and contact information of individual(s) associated with Client's OriginsNext account (e.g. billing address, email address, or name);
(iii) Users' device and connection information (e.g. IP address); and
(iv) content/description of technical support requests (excluding attachments).
OriginsNext Usage Data means Personal Data relating to or obtained in connection with the use, performance, operation, support or use of the Platform, including via their connection to Third-Party Software. OriginsNext Usage Data may include event name (i.e. what action Users performed), event timestamps, browser information, diagnostic data, data types, file sizes, and similar information associated with data from the Platform and Third-Party Software that Client connects to the Platform. For clarity, **OriginsNext Usage Data** does not include Client Personal Data.
Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Client Data means all electronic data, information, or materials, including but not limited to Client Personal Data, submitted to the Platform by or on behalf of Client or its Users.
Client Personal Data means Personal Data contained in Client Data and/or Client Materials that OriginsNext Processes under the Agreement solely on behalf of the Controller.
Client Terms means the OriginsNext Client Terms and Conditions available at https://www.originsnext.com/client-terms

Documentation means the manuals, policies, guides, instructions, or other written materials made available by OriginsNext to describe the functionality, operation, and use of the Services or Platform.

End User Terms means the terms located at www.originsnext.com/terms, as updated from time to time.
Engagement means the arrangement under which you access or use the Services, as described in an applicable Engagement Letter.
Engagement Letter means the document that records the commercial agreement between you and OriginsNext for the provision of Services. This may include a formal letter, contract, or any other document that incorporates or refers to the Client Terms and sets out the agreed scope, duration, fees, or other engagement particulars.
Personal Data means information about an identified or identifiable natural person, or which otherwise constitutes personal data, personal information, personally identifiable information or similar terms as defined in Applicable Data Protection Law.

Platform means the OriginsNext software-as-a-service (SaaS) platform and all associated systems, APIs, interfaces, modules, features, documentation, and any updates or enhancements provided by us that enable traceability, compliance, and data management across Clients and/or supply chains.
Processing (and Process) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Processor means the entity which Processes Personal Data on behalf of the Controller.
Security Incident means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Client Data Processed by OriginsNext and/or its Sub-processors.
Services means the services and Deliverables that we provide to you in connection with the Engagement Letter, and includes access to and use of the Platform where applicable.
Sub-processor means any third party, including OriginsNext Affiliates and Assisting Parties, engaged by OriginsNext to Process Client Personal Data on behalf of the Client. This includes any third-party delivery partners, contractors, suppliers, and cloud computing providers that assist OriginsNext in performing the Services, as defined in the Client Terms.

10. Schedule 1

10.1 Description of Processing

(a) Categories of data subjects whose Personal Data is Processed: Client and their respective Users.
(b) Categories of Personal Data Processed: OriginsNext Account Data, OriginsNext Usage Data, and Client Personal Data.
(c) Sensitive data transferred: None. OriginsNext Account Data and OriginsNext Usage Data do not contain data

(i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

(ii) genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, or

(iii) relating to criminal convictions and offences (altogether Sensitive Data).

(d) The frequency of the transfer: Continuous.
(e) Nature of the Processing: OriginsNext will Process Personal Data to provide the Platform and related Services in accordance with the Agreement, including this DPA. Additional information regarding the nature of the Processing (including transfer) may be described in respective Engagement Letters for the Platform and Documentation referring to technical capabilities and features, including but not limited to collection, structuring, storage, transmission, or otherwise making available of Personal Data by automated means.

10.2 Purpose(s) of the Processing:

(a) Client Personal Data: OriginsNext will Process Client Personal Data as Processor in accordance with the Controller's instructions as set out in Section 2.1 (Client Instructions).
(b) OriginsNext Account Data and OriginsNext Usage Data: OriginsNext will Process OriginsNext Account Data and OriginsNext Usage Data for the limited and specified purposes outlined in Section 1.1 (Roles of the Parties).

10.3 Duration of Processing:

(a) Client Personal Data: OriginsNext will Process Client Personal Data for the term of the Agreement as outlined in Section 6 (Deletion and Return of Client Personal Data).
(b) OriginsNext Account Data and OriginsNext Usage Data: OriginsNext will Process OriginsNext Account Data and OriginsNext Usage Data only as long as required (a) to provide Platform and related Services to the Controller in accordance with the Agreement; (b) for OriginsNext's legitimate business purposes outlined in Section 1.1 (Roles of the Parties); or (c) by applicable Law(s).

10.4 Transfers to Sub-processors:

(a) OriginsNext will transfer Client Personal Data to Sub-processors as permitted in Section 4 (Sub-processing).

11. Schedule 2

11.1 Region-Specific Terms

Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this Schedule will have the meanings given to them in Section 4 of this Schedule.

11.2 Europe, United Kingdom and Switzerland.

(a) **Client Instructions.** In addition to Section 2.1 (Client Instructions) of the DPA above, OriginsNext will Process Client Personal Data only on documented instructions from the Controller, including with regard to transfers of such Client Personal Data to a third country or an international organisation, unless required to do so by Applicable Data Protection Law to which OriginsNext is subject; in such a case, OriginsNext shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. OriginsNext will promptly inform the Controller if it becomes aware that the Controller's Processing instructions infringe Applicable Data Protection Law.

(b) **European Transfers**. Where Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

(i) The EU SCCs are hereby incorporated into this DPA by reference as follows:

(A) The Controller (the Client) is the data exporter and OriginsNext is the data importer.

(B) Module One (Controller to Controller) applies where OriginsNext is Processing OriginsNext Account Data or OriginsNext Usage Data.

(C) Module Two (Controller to Processor) applies where Client is a Controller of Client Personal Data and OriginsNext is Processing Client Personal data as a Processor.

(D) Module Three (Processor to Processor) applies where Client is a Processor of Client Personal Data and OriginsNext is Processing Client Personal Data as another Processor.

(E) By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

(ii) For each Module, where applicable:

(A) In Clause 7, the optional docking clause does not apply.

(B) In Clause 9, Option 2 applies, and the time period for prior notice of Sub-processor changes is stated in Section 4 (Sub-processing) of this DPA.

(C) In Clause 11, the optional language does not apply.

(D) In Clause 17, Option 1 applies, and the EU SCCs are governed by the law of the EU Member State in which the Controller is established.

(E) In Clause 18(b), disputes will be resolved before the courts of the EU Member State in which the Controller is established.

(F) The Appendix of EU SCCs is populated as follows:

- The information required for Annex I(A) is located in the Agreement and/or relevant Engagement Letters.
- The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this DPA.
- The competent supervisory authority in Annex I(C) will be determined in accordance with the Applicable Data Protection Law; and

- The information required for Annex II is located in Schedule 4 (Technical and Organisational Security Measures).

(c) **Swiss Transfers**. Where Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in Section 11.2(b) (European Transfers) above with the following modifications:

(i) All references in the EU SCCs to Regulation (EU) 2016/679 will be interpreted as references to the Swiss FADP, and references to specific Articles of Regulation (EU) 2016/679 will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this DPA will be interpreted as references to the FADP.

(ii) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

(iii) In Clause 17, the EU SCCs are governed by the laws of Switzerland.

(iv) In Clause 18(b), disputes will be resolved before the courts of Switzerland.

(v) All references to Member State will be interpreted to include Switzerland and Data Subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

(d) **United Kingdom Transfers**. Where Personal Data protected by the UK Data Protection Law is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

(i) The EU SCCs apply as set forth in Section 11.2(b) (European Transfers) above with the following modifications:

(A) Each party shall be deemed to have signed the UK Addendum.

(B) For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant Engagement Letters.

(C) For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule.

(D) For Table 3 of the UK Addendum:

- The information required for Annex 1A is located in the Agreement and/or relevant Engagement Letters.
- The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA.
- The information required for Annex II is located in Schedule 4 (Technical and Organisational Security Measures).
- The information required for Annex III is located in Section 4 (Sub-processing) of this DPA.

(ii) In Table 4 of the UK Addendum, both the data importer and data exporter may end the UK Addendum.

11.3 **United States of America**. The following terms apply where OriginsNext Processes Personal Data subject to the US State Privacy Laws:

(a) To the extent Client Personal Data includes personal information protected under US State Privacy Laws that OriginsNext Processes as a Service Provider or Processor, on behalf of Client, OriginsNext will Process such Client Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Client's written instructions, as necessary for the limited and specified purposes identified in Section 1.1(a) (Client Personal Data) and Schedule 1 (Description of Processing) of this DPA. OriginsNext will not:

(i) retain, use, disclose or otherwise Process such Client Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related Engagement Letter, or as otherwise permitted under US State Privacy Laws;

(ii) sell or share such Client Personal Data within the meaning of the US State Privacy Laws; and

(iii) retain, use, disclose or otherwise Process such Client Personal Data outside the direct business relationship with Client and not combine such Client Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

(b) OriginsNext must inform Client if it determines that it can no longer meet its obligations under US State Privacy Laws within the timeframe specified by such laws, in which case Client may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorised Processing of such Client Personal Data.

(c) To the extent Client discloses or otherwise makes available Deidentified Data to OriginsNext or to the extent OriginsNext creates Deidentified Data from Client Personal Data, in each case in its capacity as a Service Provider, OriginsNext will:

(i) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that OriginsNext may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and

(iii) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons (Recipients), contractually obligate any such Recipients to comply with all requirements of this Section 2.3 (including imposing this requirement on any further Recipients).

11.4 Region Specific Definitions

(a) Where Personal Data is subject to the laws of one the following regions, the definition of Applicable Data Protection Law includes:

(i) Argentina: The Personal Data Protection Law;

(ii) Australia: the Australian Privacy Act;

(iii) Brazil: the Brazilian Lei Geral de Proteção de Dados (General Personal Data Protection Act, Law No. 13,709/2018);

(iv) Canada: the Canadian Personal Information Protection and Electronic Documents Act;

(v) Chile: The Personal Data Protection Bill;

(vi) Colombia: The Law 1581 of 2012;

(vii) Europe: (i) the 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, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time (EU Data Protection Law);

(viii) Japan: the Japanese Act on the Protection of Personal Information;

(ix) Singapore: the Singapore Personal Data Protection Act;

(x) Switzerland: the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time (Swiss FADP);

(xi) The United Kingdom: the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time (UK Data Protection Law); and

(xii) The United States: all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations (CCPA), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act (US State Privacy Laws).

(xiii) Uruguay: Law No. 18.331 on the Protection of Personal Data and the Habeas Data Action.

(b) De-identified Data means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

(c) Data Privacy Framework means the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework self-certification program operated by the US Department of Commerce.

(d) Europe includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

(e) EU SCCs means 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 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

(f) Service Provider has the same meaning as given in the CCPA.

(g) UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

12. Schedule 3

12.1 Sub-processors

(a) Effective Starting 15 July 2026

12.2 Third-Party Sub-processors

(a) OriginsNext uses the third-party entities listed below (each, a "Sub-processor") to process Client Personal Data on behalf of OriginsNext Clients in accordance with agreements between OriginsNext and the Sub-processor to uphold OriginsNext's commitments in OriginsNext's Data Processing Addendum. Defined terms, such as "Personal Data", "Client Personal Data", "Sub-processor", "Platform", or "End User Personal Data" have the same meaning as in OriginsNext's Data Processing Addendum, or OriginsNext's Client Terms Agreement, as the case may be.

(b) OriginsNext carries out periodic compliance reviews of its Sub-processors, and where the engagement of a Sub-processor requires the cross-border transfer of Personal Data, OriginsNext conducts Transfer Impact Assessments in accordance with Applicable Data Protection Law for these data transfers. OriginsNext imposes obligations on its Sub-processors to implement appropriate technical and organisational measures ensuring that the sub-processing of Personal Data is protected to the standards required by Applicable Data Protection Law and the same standard provided by OriginsNext's Data Processing Addendum.

(c) The list below contains Sub-processors for each of OriginsNext's Platform and related Services. For each Sub-processor below, processing of Personal Data will be for the duration of use of the applicable service(s) by the Controller, and for the retention periods as set out in the Client Terms, Engagement Letter or any product documentation. Further information about Sub-processor security measures can be found via the external links below.

Sub-Processor	Nature And Purpose Of Processing	Categories Of Personal Data	Location Of Processing	Security Measures
Microsoft Corporation	Cloud hosting provider	OriginsNext Account Data, OriginsNext Usage Data, and Client Personal Data	Australia	Microsoft Trust Centre
Intercom	Client Help Centre and support ticketing provider	OriginsNext Account Data, and Client Personal Data	USA	Intercom Security & Privacy
Google Analytics	Analytics to help us improve your Platform experience	OriginsNext Usage Data	USA	Privacy Controls in Google Analytics
Harness	Feature access and release management	OriginsNext Account Data, and Client Personal Data	USA	Harness Trust Centre

Sub-Processor	Nature And Purpose Of Processing	Categories Of Personal Data	Location Of Processing	Security Measures
Pipedrive	Customer Relationship Management (CRM) solution	OriginsNext Account Data, and Client Personal Data	Australia	Pipedrive Privacy
Webflow	Public website and contact form hosting service	OriginsNext Account Data, and Client Personal Data	USA	Webflow Global Privacy

13. Schedule 4

13.1 Technical and Organisational Security Measures

OriginsNext maintains a formal Information Security Policy to protect the confidentiality, integrity, and availability of information across its operations. The policy establishes a framework for managing security risks and ensuring compliance with applicable laws and regulations. A comprehensive copy of this policy is available to the Controller upon request and under a non-disclosure agreement.

13.2 Security Governance and Program

(a) The Chief Technology Officer (CTO) is the designated authority responsible for the overall leadership and strategic direction of the company's information security efforts.

(b) The CTO oversees the development, implementation, and enforcement of the Information Security Policy and leads the risk management framework to identify and mitigate risks.

(c) The OriginsNext delivery team strictly follows principles of separation of duties, least privilege, mandatory code peer review, and change approval processes.

(d) Annual review of security controls and procedures based on the NIST SP 800-53 framework is conducted.

(e) Annual penetration testing for the application and infrastructure is performed by an external accredited cybersecurity team.

(f) OriginsNext is committed to maintaining compliance with national and international standards, and periodic internal and external audits are conducted to ensure this compliance.

13.3 Information Classification and Data Handling

(a) Information is classified based on its sensitivity, with specific handling procedures for each classification.

(b) Data classifications include Public, Internal, Confidential, and Restricted information. Data classifications include Public, Internal, Confidential, and Restricted information.

(c) Confidential and Restricted Information must be encrypted at rest and in transit. Confidential and Restricted Information must be encrypted at rest and in transit.

(d) Data retention policies are enforced to ensure that sensitive data is only retained for as long as necessary, and securely deleted when no longer required.

13.4 Access Control

(a) OriginsNext adheres to the principle of least privilege, ensuring users are only granted access necessary for their roles.

(b) Access provisioning follows a formal request process with manager approval.

(c) Access to systems requires proper user authentication.

(d) Multi-factor authentication (MFA) is implemented for systems holding confidential or restricted data.

(e) OriginsNext leverages Azure Active Directory B2C for Identity Lifecycle and Access Management. Single sign-on (SSO) is supported using the OIDC protocol.

(f) Role-based access control (RBAC) is used to manage user permissions within their tenant.

13.5 Data Encryption and Protection

(a) All sensitive data is protected through encryption both at rest and in transit.

(b) Strong encryption at rest is enabled by default (256-bit, FIPS 140-2 compliant).

(c) Data in transit is protected by a minimum of TLS 1.2 with strong ciphers.

(d) Azure Key Vault is used to safeguard cryptographic keys and secrets.

13.6 Incident Response and Management

(a) All employees are required to promptly report any security incidents, including suspicious activities or potential breaches.

(b) The CTO ensures a formal incident reporting procedure is in place, and all incidents are documented, investigated, and mitigated.

(c) An Incident Response Team (IRT) is established to manage and coordinate responses to significant incidents.

(d) Root cause analysis is conducted after each incident to improve security practices.

13.7 Business Continuity and Disaster Recovery

(a) Critical data and configurations are backed up regularly and stored securely offsite. Backups are encrypted through AES 256-bit encryption for data stored at rest.

(b) Data is backed up across multiple Australian regions for redundancy.

(c) Continuity is achieved through a combination of automated backups, auto-recovery, availability zones, geo-redundancy, and automation for cloud component provision.