DATA PROCESSING AGREEMENT

Version April 2026

This Data Processing Agreement ("DPA") is entered into by and between the Revalize entity listed in the specific Order Form ("Provider") and the entity agreeing to these terms ("Customer") (collectively "Parties" and each a "Party") and applies to the Processing of Personal Data in connection with the Parties agreement governing the provision of software and/or services by Provider to Customer ("Agreement"). This DPA forms part of the Agreement and sets out the Parties' respective rights and obligations regarding such Processing. For and in consideration of the representations and promises set forth herein, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. PROCESSING OF PERSONAL DATA

1.1. Customer on behalf of itself and each Customer Affiliate instructs Provider to Process Personal Data during the term of the Agreement and solely for the purpose of providing the Services in accordance with the Agreement and this DPA. The Data Processing Instructions sets out the subject matter and other details regarding the Processing of the Personal Data contemplated as part of the Services, including Data Subjects, categories of Personal Data, special categories of Personal Data, Sub processors and description of Processing. Additional or more specific descriptions of Processing activities may be included in the Agreement.

1.2. Provider may Process Personal Data, depending on the Services, for the following purposes: hosting and storage; backup and disaster recovery; service change management; incident and issue resolution; applying new product or system versions, patches, updates, and upgrades; monitoring and testing system use and performance; IT security (including threat detection, incident management, and access control); maintenance and operation of technical support systems and IT infrastructure; and migration, implementation, configuration, and performance testing of the Services.

1.3. As part of the provision of the Services, and depending on the specific Services contracted, Provider may Process Personal Data relating to Customer's individuals, including Customer's end users, employees, job applicants, contractors, collaborators, partners, suppliers, customers, and clients.

1.4. The Parties acknowledge that Customer's transfer or disclosure of Personal Data to Provider is not a "sale" of Personal Data within the meaning of applicable Privacy Laws (including the CCPA) and Provider provides no monetary or other valuable consideration to Customer in exchange for the Personal Data.

1.5. Unless otherwise expressly specified in the Agreement, Customer may not provide Provider with sensitive data or any data that imposes specific data security, data protection or regulatory obligations on Provider in addition to or different from those specified in this DPA.

1.6. Provider will not (i) retain, use, disclose or otherwise Process Personal Data for any purpose (including its own commercial purposes) other than on Customer's documented instructions (as set out in this DPA and in the Agreement) unless Processing is required under applicable law and under the terms of the Standard Contractual Clauses (where applicable); or (ii) sell Personal Data received from customer or obtained in connection with the provision of the Services to Customer.

1.7. The additional terms set forth in Annex VI apply to the extent the CCPA applies to the Customer.

2. PROVIDER PERSONNEL

Provider shall ensure that all its personnel authorized to Process Personal Data are: committed to confidentiality or under an appropriate statutory obligation of confidentiality with respect to such Personal Data; and (ii) have received appropriate training regarding the protection of Personal Data.

3. SECURITY

3.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall in relation to the Personal Data implement appropriate technical and organizational measures designed to provide a level of security appropriate to that risk in the provision of the Services. For the purposes of this DPA, Provider's technical and organizational measures are set forth in the Information Security Schedule.

3.2. In assessing the appropriate level of security, Provider shall consider, in particular, the risks posed by the Processing of Personal Data.

4. SUBPROCESSING

4.1. Provider shall only appoint Sub processors that enable Provider to comply with applicable Privacy Laws. Customer hereby authorizes Provider to appoint Sub processors in accordance with this Section 4, subject to any restrictions or conditions expressly set forth in this DPA. Consistent with Annex III, Customer consents to the Sub processors in the Subprocessors list (available at Revalize Subprocessors List) as of the effective date of this DPA and any new Sub processors as set forth in Section 4.2. As required by applicable Privacy Laws, Provider will enter into an appropriate written contract with each such Sub processor. Provider remains liable to Customer for its Sub processors' performance under this DPA.

4.2. Notwithstanding any notice requirements in this DPA, before Provider engages any new Sub processor, Provider shall give Customer notice of such appointment, including details of the Processing to be undertaken by the proposed Sub processor. Any new Sub processor shall be added to the Subprocessors list (available at Revalize Subprocessors List) and notification sent to Customer via email or other reasonable electronic means. In addition to any other notifications, Provider may provide such notice by updating the Subprocessors list in our website. Customer may notify Provider of any objections (on reasonable grounds related to Privacy Laws) to the proposed Sub processor or Data Processing Instructions ("Objection"), within 15 days of the notification from Provider of the updated Subprocessors list, then Provider and Customer shall negotiate in good faith to agree to further measures including contractual or operational adjustments relevant to the appointment of the proposed Sub processor or operation of the Services to address Customer's Objection. Where such further measures cannot be agreed between the Parties within forty-five (45) days from Provider's receipt of the Objection (or such greater period agreed by Customer in writing), Customer may by written notice to Provider with immediate effect terminate that part of the Services which require the use of the proposed Sub processor or another part of the Services which are so terminated.

5. DATA SUBJECT RIGHTS.

Provider shall:

5.1. Upon becoming aware, promptly notify Customer if Provider receives a request from a Data Subject relating to an actionable Data Subject right under any applicable Privacy Law in respect of Personal Data;

5.2. Not respond to that request except on the documented instructions of Customer or as required by a Supervisory Authority or under applicable law; and

5.3. Upon request from Customer where required by Privacy Laws and in the context of the Services, reasonably assist Customer in dealing with an actionable Data Subject rights request to the extent Customer cannot fulfil this request without Provider's assistance. Provider may fulfil this request by making available functionality (at Customer's expense) that enables Customer to address such Data Subject rights request without additional Processing by Provider. To the extent such functionality is not available, in order for Provider to provide such reasonable assistance, Customer must communicate such request in writing to Provider providing sufficient information to enable Provider (at Customer's expense) to pinpoint and subsequently amend, export or delete the applicable record(s).

6. PERSONAL DATA BREACH.

6.1. Provider shall notify Customer without undue delay upon Provider or any Sub processor confirming a Personal Data Breach, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under applicable Privacy Laws. Subject to Section 6.3 below, such notification shall as a minimum:

a) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

b) communicate the name and contact details of Provider's data protection officer or other relevant contact from whom more information may be obtained;

c) describe the likely consequences of the Personal Data Breach in so far as Provider is able to ascertain having regard to the nature of the Services and the Personal Data Breach; and

d) describe the measures taken or proposed to be taken to address the Personal Data Breach.

6.2. Provider shall co-operate with Customer and take such commercially reasonable steps as are necessary to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

6.3. Where and in so far as, it is not possible to provide the information or provider is prohibited by law or law enforcement from providing the information referred to in Section 6.1 at the same time, the information may be provided in phases without undue further delay.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

To the extent necessary, Provider shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which customer reasonably considers to be required by Privacy Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Provider. To the extent that such impact assessment and/or prior consultation requires assistance beyond Provider providing the applicable Provider processing record(s) and Documentation, Provider shall reserve the right to charge Customer such engagement at Provider's then current daily rates.

8. DELETION OR RETURN OF PERSONAL DATA.

8.1. Within thirty (30) days from termination or expiry of the Agreement (the "Return Period"), and subject to Section 8.2 below, at Customer's request, Provider will either delete or return available Personal Data. At the expiry of the Return Period, if Customer has not elected either of the foregoing Provider may delete and destroy all Personal Data without notice or liability to Customer. Where Customer requests Provider return available Personal Data, Provider may fulfil this request by making available functionality that enables Customer to retrieve the Personal Data without additional Processing by Provider. If Customer declines to use this functionality, Customer may, within the Return Period, request that Provider return the available Personal Data under an order for the applicable professional services. In the event the Agreement is terminated for Customer's breach, Provider shall have the right to require that Customer prepay for such professional services. Provider shall provide written confirmation to Customer that it has fully complied with this Section 8 within thirty (30) days of customer's request for such confirmation.

8.2. Provider may retain Personal Data to the extent required by Privacy Laws or any other statutory requirement to which Provider is subject and only to the extent and for such period as required by Privacy Laws or any other statutory requirement to which Provider is subject and always provided that (i) during such retention period the provisions of this DPA will continue to apply, (ii) that Provider shall ensure the confidentiality of all such Personal Data, and (iii) Provider shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Privacy Laws requiring its storage or any other statutory requirement to which Provider is subject and for no other purpose.

9. REVIEW, AUDIT AND INSPECTION RIGHTS.

9.1. Upon Customer's reasonable request, Provider shall provide all relevant and necessary information to demonstrate its compliance with appliable Privacy Laws, including such relevant and necessary information regarding Provider's technical and organizational security measures used to protect the Personal Data in relation to the Services provided. Such information may be provided in summary form to minimize the risk of such measures being circumvented.

9.2. Provider shall ensure a security audit of its technical and organizational security measures is carried out at least annually in compliance with applicable Privacy Laws. The results of such security audit will be documented in a summary report. Provider shall promptly provide Customer upon request with: (i) a confidential summary of such report; and (ii) evidence of appropriate remediation of any critical issues within four (4) weeks from date of issuance of the audit report.

9.3. If, following the completion of the steps set out in Sections 9.1 and 9.2, Customer reasonably believes that Provider is non-compliant with applicable Privacy Laws, Customer may request that Provider make available, either by webinar or in a face-to-face review, extracts of all relevant information necessary to further demonstrate compliance with applicable Privacy Laws. Customer undertaking such review shall give Provider reasonable notice, by contacting Provider's Data Privacy Team at dpo@revalizesoftware.com, and any review will be conducted as set forth under this Section 9.3.

9.4. In the event that Customer reasonably believes that its findings following the steps set forth in Section 9.3 do not enable Customer to materially comply with Customer's obligations mandated under applicable Privacy Laws in relation to its appointment of Provider, then Customer may give Provider not less than thirty (30) days prior written notice of its intention to undertake an audit, which may include inspections of Provider to be conducted by Customer or an auditor mandated by Customer (not being a competitor of Provider). Such audit and/or inspection shall: (i) be subject to confidentiality obligations agreed between Customer (or its mandated auditor) and Provider, (ii) be undertaken solely to the extent mandated by, and may not be further restricted under applicable Privacy Laws, (iii) not require Provider to compromise the confidentiality of security aspects of its systems and/or data processing facilities (including that of its Sub processors), and (iv) not be undertaken where it would place Provider in breach of Provider's confidentiality obligations to other Provider customers, vendors and/or partners generally or otherwise cause Provider to breach laws applicable to Provider. Customer (or auditor mandated by Customer) undertaking such audit or inspection shall avoid causing any damage, injury or disruption to Provider's premises, equipment, personnel and business in the course of

such a review. To the extent that such audit performed in accordance with this Section 9.4 exceeds one (1) business day, Provider shall reserve the right to charge Customer for each additional day at its then current daily rates.

9.5. If following such an audit or inspection under Section 9.4, Customer, acting reasonably, determines that Provider is non-compliant with applicable Privacy Laws then Customer will provide details thereof to Provider upon receipt of which Provider shall provide its response and to the extent required, a draft remediation plan for the mutual agreement of the Parties (such agreement not to be unreasonably withheld or delayed; the mutually agreed plan being the "Remediation Plan"). Where the Parties are unable to reach agreement on the Remediation Plan, or in the event of agreement, Provider materially fails to implement the Remediation Plan by the agreed upon dates which in either case is not cured within forty-five (45) days following Customer's notice or another period as mutually agreed between the Parties, Customer may terminate the Services in part or in whole which relates to the non-compliant Processing and the remaining Services shall otherwise continue unaffected by such termination.

9.6. The rights of Customer under this Section 9 shall only be exercised once per calendar year unless Customer reasonably believes Provider to be in material breach of its obligations under either this DPA or applicable Privacy Laws.

10. RESTRICTED TRANSFERS.

10.1. Customer (as "data exporter") and Provider, as appropriate, (as "data importer") hereby agree that the applicable Standard Contractual Clauses shall apply in respect of any Restricted Transfer from Customer or any Customer Affiliate to Provider to the extent required by Privacy Laws. The Parties agree that the provisions of the Standard Contractual Clauses shall apply to the Restricted Transfer. Where Personal Data is subject to the EU GDPR, the applicable Standard Contractual Clauses shall be the EU SCCs, and where Personal Data is subject to the UK GDPR, the applicable Standard Contractual Clauses shall be the UK Addendum, in each case completed as described herein and as set out in the Annexes. Where Personal Data is subject to Swiss Federal Data Protection Act, the provisions of the Swiss Addendum shall apply.

10.2. For the purposes of Annex I or other relevant part of the applicable Standard Contractual Clauses, the Data Processing Instructions sets out the Data Subjects, categories of Personal Data, special categories of Personal Data, Sub processors and description of Processing (processing operations). Where the EU SCCs apply to transfers from the Customer or a Customer Affiliate to Provider, they will be completed as set out in Annex I. Optional clauses in the applicable Standard Contractual Clauses shall not apply unless otherwise set out in Annex I.

10.3. For the purposes of Annex II or other relevant part of the applicable Standard Contractual Clauses, the Information Security Schedule sets out the description of the technical and organizational security measures implemented by provider (the data importer).

10.4. Provider shall not make any Restricted Transfer of Personal Data that it has received under this DPA, unless it has lawful grounds to do so under applicable Privacy Laws. Such lawful grounds may include (i) an Adequacy Decision, (ii) Standard Contractual Clauses, (iii) the terms of other recognized forms of data transfer agreements or processes); or (iv) any permitted derogation under Privacy Law.

11. Liability

TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW, ALL THE LIMITATIONS AND EXCLUSIONS OF LIABILITY SET FORTH IN THE AGREEMENT, INCLUDING WITHOUT LIMITATION ANY LIABILITY FOR DATA PROTECTION CLAIMS BETWEEN THE PARTIES, SHALL ALSO APPLY IN RESPECT TO THIS DPA. This contractual allocation and limitation of liability shall apply only to the internal relationship between the Parties and shall not limit or exclude any mandatory liability of either Party towards data subjects or third parties under the GDPR or other applicable Privacy Laws, including data subjects' rights to full and effective compensation under Article 82 GDPR.

12. OTHER PRIVACY LAWS.

12.1. To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements or introduces any such requirements in the future, in addition to those in this DPA, both Parties may agree to any additional measures required to ensure compliance with applicable Privacy Laws and any such additional measures agreed to by the Parties will be documented as an Annex to this DPA or in an order to the Agreement.

12.2. The Customer further agrees that to the extent that provider is required to enter into an appropriate transfer mechanism or additional safeguards to transfer Personal Data under applicable Privacy Laws, Provider may enter into an agreement to affect such a transfer on its own behalf, and where required on behalf of Customer, on a named or unnamed basis.

12.3. Due to the fact that Provider has no control over the type, character, properties, content, and/or origin of Personal Data Processed hereunder, notwithstanding anything to the contrary herein, Provider shall not be in breach of this DPA or the

Agreement or liable to Customer to the extent Personal Data subject to jurisdictional requirements mandating security, Processing or other measures not set forth in, or contrary to the terms of, this DPA is provided by Customer without amending this DPA or entering into an order addressing the same.

12.4. If any variation is required to this DPA as a result of a change in Privacy Laws, including any variation which is required to the Standard Contractual Clauses, then either Party may provide written notice to the other Party of that change in law. The Parties will discuss and negotiate in good faith any necessary variations to this DPA, including the Standard Contractual Clauses, to address such changes.

13. GENERAL TERMS.

13.1. This DPA shall be governed by and construed in accordance with the laws of where Customer is domiciled. The Parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply in any respect to this DPA or the Parties.

- If Customer is domiciled in any country in Europe, the governing law for this DPA shall be Germany and the courts in Germany will have exclusive jurisdiction.
- If Customer is domiciled in the US, the governing law of this DPA shall be Delaware law, and the courts of Delaware shall have exclusive jurisdiction.
- If Customer is domiciled in the United Kingdom, the governing law for this DPA shall be United Kingdom and the court in United Kingdom will have exclusive jurisdiction.
- If Customer is domiciled in any other country outside Europe or United Kingdom, the governing law for this DPA shall be Germany, and the court in Karlsruhe will have exclusive jurisdiction.

14. ORDER OF PRECEDENCE.

Nothing in this DPA reduces Provider's or any Provider Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Provider or any Provider Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of inconsistencies between the provisions of this DPA and (i) the Information Security Schedule, or (ii) any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

15. SEVERANCE.

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

16. DEFINITIONS.

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

- Adequacy Decision means, for a jurisdiction with Privacy Laws that have data transfer restrictions, a decision that the Supervisory Authority or other body in such jurisdiction recognizes as providing an adequate level of data protection as required by such jurisdiction's Privacy Laws such that transfer to that country shall be permitted without additional requirements.
- Affiliate means any entity which now or in the future controls, is controlled by, or is under common control with a Party to this DPA, with "control" defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through the ownership of voting securities, by contract, or otherwise.
- CCPA means the California Consumer Privacy Act of 2018, codified at Cal. Civ. Code § 1798.100 et seq. and as amended by the California Privacy Rights Act, and its implementing regulations, as may be further amended in the future.
- 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 including "business" as that term is defined by the CCPA, and in the context of this DPA shall mean Customer;
- Data Processing Instructions means the Processing instructions set out in Annex I(2) (Description of Transfer).
- Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller (including "service provider" as that term is defined by the CCPA), and in the context of this DPA shall mean Provider.

- Data Subject means the identified or identifiable person to whom Personal Data relates (including "consumer" as that term is defined by the CCPA).
- EU GDPR means all EU regulations applicable (in whole or in part) to the Processing of Personal Data such as Regulation (EU) 2016/679.
- EU SCCs means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on Standard Contractual cClauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council and set out as Annex I to this DPA.
- Information Security Schedule means the information security, technical and organizational measures specified in Annex II, as may be updated from time to time.
- Personal Data or Personal Information means any information relating to an identified or identifiable natural person, as defined by applicable Privacy Laws.
- Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- Privacy Laws means all data protection and privacy laws and regulations applicable to the Personal Data at issue. Without limiting the foregoing, Privacy Laws include, as applicable, the EU GDPR, UK GDPR and U.S. state privacy laws and any other similar foreign, national or regional data protection or privacy laws, in each case as amended, superseded or replaced from time to time.
- Process or Processing means any operation or set of operations that is performed upon Personal Data in connection with the Services, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, as described in the Data Processing Instructions.
- Restricted Transfer means: **(i)** a transfer of Personal Data from Customer or a Customer Affiliate to Provider; or **(ii)** an onward transfer of Personal Data from Provider to a Sub processor, in each case, where such transfer would be prohibited by Privacy Laws in the absence of an approved method of transfer (such as (a) an Adequacy Decision, (b) Standard Contractual Clauses, (c) by the terms of other recognized forms of data transfer agreements or processes under applicable Privacy Laws or (d) a permitted derogation), or would be in breach of the terms of such an approved method of transfer or permitted derogation.
- Services means the services and other activities to be supplied to or carried out by or on behalf of Provider for Customer pursuant to the Agreement.
- Standard Contractual Clauses means the contractual clauses approved by a Supervisory Authority pursuant to Privacy Laws, as may be updated from time to time, which permit the transfer of Personal Data where such transfer would otherwise be a Restricted Transfer.
- Sub processor means any third party (including any third party and any Provider Affiliate) appointed by or on behalf of Provider to undertake Processing in connection with the Services, the categories of which are set forth in Annex III and listed in the Subprocessors list available at Revalize Subprocessors List.
- Supervisory Authority means a public authority or government or quasi-governmental agency which is established in a jurisdiction under Privacy Laws with competence in matters pertaining to data protection.
- Swiss Addendum means the addendum to the EU SCCs set out in Annex III to this DPA.
- UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the UK Data Protection Act 2018, as may be amended or replaced from time to time.
- UK GDPR means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018. References to Annexes are to annexes of the EU SCCs.

DPA Annex

The annexes to this DPA are available at the following link: https://revalizesoftware.com/Legal/Revalize-DPA-Annexes-2026-April-EN.pdf.