Benelinx
Data Processing Agreement

Last Updated: March 17, 2026

This Data Processing Agreement ("**DPA**") forms part of the Benelinx Terms of Service between you ("**Customer**") and Benelinx, LLC ("**Provider**") for the purchase of access to Provider's cloud service platform (the "**Service Platform**") and related technical support by Customer (as amended from time to time, the "**Agreement**"). Capitalized terms not defined herein are defined in the Agreement, and if not defined in the Agreement, then (to the extent applicable) have the meanings set forth in the Colorado Privacy Act, C.R.S. § 6-1-1301 et seq.

This DPA is intended to ensure the protection and lawful processing of Personal Data in accordance with Applicable Data Protection Laws (as defined below), including, where applicable, the Colorado Privacy Act, C.R.S. § 6-1-1301 et seq. and Colorado's data security breach notification law, C.R.S. § 6-1-716.

1. DEFINITIONS. For the purposes of this Agreement, the following terms have the following meanings:

1.1 "**Agreement**" means the Agreement between Customer and Provider for the provision of the Service Platform and related services.

1.2 "**Applicable Data Protection Laws**" means all U.S. federal, state, and local, and other legal requirements applicable to the Processing of Personal Data under the Agreement, including, where applicable: (a) the Colorado Privacy Act, C.R.S. § 6-1-1301 et seq., and implementing rules; (b) Colorado's Notification of Security Breach statute, C.R.S. § 6-1-716; and (c) any amendments, rules, or successor provisions to the foregoing.

1.3 **"Authorized Users**" means individuals authorized by Customer to use the Service Platform under the Agreement.

1.4 "**Controller**," "**Processor**," "**Personal Data**," "**Processing**," "**Sensitive Data**," and "**Sell/Sale**" have the meanings set forth in the Colorado Privacy Act, to the extent Applicable Data Protection Laws include the Colorado Privacy Act.

1.5 "**Data Subject**" has the meaning set forth in GDPR only to the extent GDPR applies to the Parties' Processing.

1.6 "**GDPR**" means Regulation (EU) 2016/679 (General Data Protection Regulation), to the extent applicable to the Parties' Processing.

1.7 "**Sub-processor**" means any third party engaged by Processor to process Personal Data on behalf of Controller.

2. ROLES OF THE PARTIES. The Parties acknowledge and agree that, with regard to the Processing of Personal Data, Customer acts as the Controller and Provider acts as the Processor. Processor shall not determine the purposes and means of Processing of Personal Data and will not process Personal Data for any purpose other than providing the Services, except as permitted by Applicable Data Protection Laws.

3. SUBJECT MATTER, DURATION, NATURE, AND PURPOSE OF PROCESSING

3.1 **Subject Matter.** The Processing of Personal Data as necessary to provide the Service Platform and related services under the Agreement.

3.2 **Duration.** For the term of the Agreement and any applicable retention period as required by law or this DPA.

3.3 **Nature and Purpose.** The Processing is limited to what is necessary to provide the Service Platform, including hosting, storage, support, maintenance, and related activities.

3.4 **Types of Personal Data.** Limited to the categories of Personal Data that Customer (or its Authorized Users) submits to the Services. Personal Data may include identifiers and employment-related information and may include Sensitive Data (for example, data revealing health information in connection with employee benefits administration) to the extent provided by Customer.

3.5 **Categories of Data Subjects.** Customer's employees, contractors, agents, Customer's clients and other individuals whose Personal Data is provided to Provider in connection with the Services.

4. OBLIGATIONS OF THE PROCESSOR. Processor shall:

4.1 Process Personal Data only on documented instructions from Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law. In such case, Processor shall inform Controller of that legal requirement before Processing, unless prohibited by law.

4.2 Ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.3 Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Applicable Data Protection Laws.

4.4 Assist Controller, taking into account the nature of Processing and the information available to Processor, by appropriate technical and organizational measures, insofar as reasonably possible, to enable Controller to respond to Consumer requests to exercise rights under Applicable Data Protection Laws..

4.5 Assist Controller in ensuring compliance with Controller's obligations under Applicable Data Protection Laws, including with respect to security, breach notification, data protection impact assessments, and prior consultations with supervisory authorities.

4.6 At Controller's choice, delete or return all Personal Data to Controller after the end of the provision of Services relating to Processing, and delete existing copies unless applicable law requires storage of the Personal Data.

4.7 Provide Controller information reasonably necessary to enable Controller to conduct and document any data protection assessments required under Applicable Data Protection Laws, including the Colorado Privacy Act.

4.8 Make available to Controller all information necessary to demonstrate compliance with the obligations set forth in this DPA and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller, provided that such audits are subject to reasonable advance notice and confidentiality obligations. Audits may be conducted no more than once in any twelve (12) month period unless a Personal Data Breach or material non-compliance is suspected and shall be conducted during regular business hours in a manner that minimizes disruption to Processor's business operations.

5. SUB-PROCESSORS.

5.1 Controller authorizes Processor to engage Sub-processors as necessary to provide the Services. Processor will (a) maintain and make available an up-to-date list of Sub-processors at: https://benelinx.com/legal/subprocessors; and (b) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set forth in this DPA with respect to the Personal Data processed.

5.2 Processor shall provide Controller with advance notice of any intended changes concerning the addition or replacement of Sub-processors, thereby giving Controller the opportunity to object on reasonable grounds. Any objection must be made in writing within ten (10) business days after notice and must describe reasonable grounds relating to data protection. If the Parties cannot resolve the objection, Customer may terminate the affected Services without penalty (and receive a pro-rated refund of prepaid fees for the terminated portion, if any).

5.3 For the avoidance of doubt, a Third-Party Service Provider is not a Sub-processor of Provider unless Provider has engaged that Third-Party Service Provider to process Personal Data on Provider's behalf. Where Customer directs Provider to enable a data connection to a Third-Party Service Provider selected by Customer, that Third-Party Service Provider

processes data as Customer's own processor or as an independent controller, and Customer is responsible for entering into an appropriate data processing agreement with such Third-Party Service Provider.

6. INTERNATIONAL DATA TRANSFERS. Processor may process Personal Data in the United States and other jurisdictions where Processor or its Sub-processors operate, subject to the safeguards required by Applicable Data Protection Laws. To the extent GDPR applies, the Parties will rely on an appropriate transfer mechanism (for example, Standard Contractual Clauses) for restricted transfers.

7. DATA SECURITY AND BREACH NOTIFICATION.

7.1 Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Processor's security measures are detailed here, which may be amended from time to time in the Processor's sole discretion: [add URL for your security measures]

7.2 Processor shall notify Controller without undue delay, and in any event within seventy-two (72) hours after confirming a Personal Data Breach affecting Controller Personal Data, and will provide information reasonably required for Controller to comply with Applicable Data Protection Laws. Processor will cooperate in good faith with Controller's investigation, mitigation, and notifications, including obligations under C.R.S. § 6-1-716.

8. DATA SUBJECT RIGHTS. Processor shall promptly notify Controller if it receives a request from a Consumer or Data Subject to exercise rights under Applicable Data Protection Laws. Processor shall not respond to such request except on Controller's documented instructions or as required by law.

9. LIABILITY. The liability of each Party under this DPA shall be subject to the limitations and exclusions of liability set forth in the Agreement, except as otherwise required by Applicable Data Protection Laws. Nothing in this DPA is intended to waive or limit any Party's obligations that cannot be waived or limited under Applicable Data Protection Laws.

10. TERM AND TERMINATION. This DPA shall remain in effect for as long as Processor processes Personal Data on behalf of Controller under the Agreement.

11. GOVERNING LAW AND JURISDICTION. This DPA shall be governed by and construed as specified in the Agreement, and any disputes arising under this DPA shall be subject to the exclusive jurisdiction of the courts specified in the Agreement.

12. MISCELLANEOUS.

12.1 In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall prevail with respect to the subject matter herein.

12.2 This DPA may be amended by Provider upon at least thirty (30) days' prior written notice to Customer. Customer may reject any amendment by providing Provider written notice of rejection before the effective date of the amendment, in which case the Parties will continue to be governed by the version of this DPA in effect immediately prior to the rejected amendment with respect to Customer's use of the Service Platform, unless the Agreement is terminated in accordance with its terms.