beeline®

Client Data Protection Addendum
(Controller:Processor)

I. Introduction

The undersigned, Beeline.com, LLC for and on behalf of itself and its Affiliates, (collectively, "Beeline") and you, for and on behalf of yourself and your Affiliates (collectively, "Client") agree to the terms of this Data Protection Addendum ("DPA") which sets forth our obligations with respect to the processing and security of Client Data in connection with the Services provided by Beeline to Client, (collectively, the "Parties") in conjunction with the terms and conditions entered into between the Parties for the Services. Such terms and conditions and any other terms set out by Beeline in conjunction with the Services, including without limitation any of Beeline's terms of use, sales orders, service orders, statements of work and terms for professional services, shall be collectively referred to as the "Agreements." The DPA is deemed incorporated by reference into the Agreements. The provision of third-party products and services made available to Client via the Platform are governed by separate terms provided to Client, including different privacy and security terms as provided by such third party.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in the Agreements, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Beeline Privacy Notice that otherwise may apply to processing of Client Data as defined herein.

II. Definitions

The following defined terms are used in this DPA:

"Affiliate" means, (i) in the case of Beeline, any entity controlled by Beeline.com, LLC, and (ii) in the case of Supplier, any entity controlled by Supplier. For purposes of the preceding sentence, "control" means the direct or indirect ownership of more than 50% of the voting interests of an entity.

"CCPA" means the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act.

"Client Data" means all data, including all text, sound, video, or image files Client uploads into the Platform including any data that is uploaded into the Platform by Client's agents or its users on their behalf. Client Data also includes Client's Personal Data that is Client Data.

"Data Protection Requirements" means the GDPR, Local EU/EEA/Switzerland Data Protection Laws, the Swiss Federal Act on Data Protection in effect as of September 1, 2023, the UK Data Protection Act 2018, CCPA and any other applicable laws, regulations, and other legal requirements relating to privacy and data security.

"DPA Terms" means the terms in this DPA.

"EEA" means the European Economic Area.

"EU" means the European Union.

"EU Adequacy Decision" means the adequacy decision adopted on July 10, 2023 by the European Commission for the EU-U.S. DPF.

"EU-U.S. DPF" means the EU-U.S. Data Privacy Framework is the data privacy framework launched by the U.S. Department of Commerce on July 10, 2023, which serves as an approved method of data transfers from the EU to the United States.

"EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"GDPR" means the EU GDPR and the UK GDPR collectively.

"Local EU/EEA/Switzerland Data Protection Laws" means any legislation and regulation implementing the GDPR.

"Non-Beeline Products" shall mean any third-party products or services made available to Client ancillary to the Services whether via the Platform or otherwise and are subject to the third-party's terms of use, data protection terms and privacy policy, where such third-party products or services are selected by Client and Client accepts such third-party terms.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Platform" shall mean Beeline's Extended Workforce Platform, Vendor Management System or other cloud-based solution with applications and features as more fully described in one or more service orders or statements of work and Beeline's documentation.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data. Security Incident also includes any personal data breach as defined by the GDPR. A Security Incident does not include any activity which does not result in unauthorized access to Client Data including without limitation, denial of service and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful login attempts, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

"Service(s)"mean(s) the SaaS services and associated professional services and documentation provided in conjunction with the Platform excluding Non-Beeline Products.

"Sub-processor" means other processors used by Beeline to process Supplier Data, as described in Article 28 of the GDPR.

"UK Extension to the EU-U.S. DPF" means the approved data transfer mechanism issued by the UK to permit the transfer of Personal Data from the UK (and Gibraltar) to the United States under the UK GDPR, effective October 12, 2023.

"UK GDPR" means the General Data Protection Regulation as incorporated into UK law by the UK Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic

Communications (Amendments etc.) (EU Exit) Regulations 2019, (each as amended, replaced, or superseded).

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, and "adequacy decision" will be subject to the requirements of Article 45(s) of the GDPR, irrespective of whether the GDPR applies.

III. DPA Terms

A. Compliance with Laws

Beeline will comply with all laws and regulations applicable to its provision of the Services including security breach notification law and Data Protection Requirements. However, Beeline is not responsible for compliance with any laws or regulations applicable to Client or Client's industry that are not applicable to SaaS providers. Beeline does not determine whether Client Data includes information subject to any such specific law or regulation.

Client must comply with all laws and regulations applicable to its use of Services including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Client is responsible for determining whether the Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Services in a manner consistent with Client's legal and regulatory obligations. Client is responsible for responding to any request from a third-party regarding Client's use of Services.

B. Scope

The DPA Terms apply to all Services except as described in this section.

The DPA Terms will not apply to any Non-Beeline Product which is governed by the privacy and security terms in the applicable Non-Beeline Product-specific terms.

For clarity, the DPA Terms apply only to the processing of Personal Data in environments controlled by Beeline and Beeline's Sub-processors. This includes Personal Data processed by Beeline when providing the Services but does not include Personal Data that remains on the premises or systems of Client or its agents or in any Client selected third-party operating environments.

C. Use of Sensitive or Restricted Data

Client is the data controller and Beeline is the data processor for the Personal Data that Client elects to upload to and utilize within Beeline's Platform. The decision to upload the Personal Data of a data subject that is subject to Data Protection Requirements of a particular country or which may be sourced from an embargoed nation, lies solely with Client. Beeline does not scan or review Client Data that Client uploads into the Platform for compatibility with Data Protection Requirements, embargoes sanctions or international trade laws. Once Personal Data has been uploaded by the Client, Beeline as the processor, will comply with the applicable Data Protection Requirements to secure the sensitive Personal Data by implementing the proper security controls to protect such Personal Data in light of the nature and scope of the processing conducted by Beeline and its Sub-processors, and will support the Client with their obligations as the controller under applicable Data Protection Requirements, as applicable to Beeline.

The Beeline Platform and Services are not designed for use with the Personal Data of minors and does not require the sharing of sensitive Personal Data. Client is solely responsible for managing the Personal Data that it provides to Beeline.

D. New Features, Supplements, or Related Software

When Beeline introduces features, offerings, supplements or related Services that are new (i.e., that were not previously included with the Services), Beeline may provide terms or make updates to this DPA that apply to Client's use of those new features, offerings, supplements or related Services. If those terms include any material adverse changes to the DPA Terms, Beeline may provide Client a choice to use the new features, offerings, supplements, or related Services, without loss of existing functionality of a generally available Service. If Client does not install or use the new features, offerings, supplements, or related Services, the corresponding new terms will not apply.

E. Government Regulation and Requirements

Beeline may modify or terminate a Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Beeline to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Beeline to continue offering the Service without modification, and/or (3) causes Beeline to believe the DPA Terms or the Service may conflict with any such requirement or obligation.

F. Electronic Notices

Beeline may provide Client with information and notices about Services and this DPA electronically, including via email, an RSS Feed, the Platform, or through a web site that Beeline identifies. Notice is given as of the date it is made available by Beeline.

G. Nature of Data Processing; Ownership

Beeline will use and otherwise process Personal Data only as described and subject to the limitations provided below: (1) to provide Client the Services in accordance with Client's documented instructions, (2) for business operations incident to providing the Services to Client; or (3) as required to meet its legal obligations.

1. Processing to Provide Client the Services

For purposes of this DPA, "to provide" a Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Client and its users, including providing personalized features;
- Troubleshooting (preventing, detecting, and repairing problems including Security Incidents);
- Ongoing improvement (installing the latest updates if and when available and making improvements to user productivity, reliability, efficacy, quality, and security); and
- Providing services ancillary to the Services.

2. Processing for Business Operations

For purposes of this DPA, "business operations" consist of the following, each as incident to delivery of the Services to Client: (a) billing and account management; (b) compensation (e.g., calculating Beeline employee commissions and partner incentives); (c) internal reporting and business modeling (e.g.,

forecasting, revenue, capacity planning, product strategy); (d) combatting fraud and cybercrime; (e) improving functionality of the Services and the Client experience; and (f) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below). Beeline will comply with its obligations, as an independent data controller, under the GDPR for such use.

H. Disclosure of Processed Data

Beeline will not disclose or provide access to any Processed Data except: (1) as Client directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: Client Data and any other data processed by Beeline in connection with the Services that is Client's confidential information under the Agreements. All processing of Processed Data is subject to Beeline's obligation of confidentiality under the Agreements.

Beeline will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Beeline with a demand for Processed Data, Beeline will attempt to redirect the law enforcement agency to request that data directly from Client. If compelled to disclose or provide access to any Processed Data to law enforcement, Beeline will promptly notify Client and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Beeline will promptly notify Client unless prohibited by law. Beeline will reject the request unless required by law to comply. If the request is valid, Beeline will attempt to redirect the third party to request the data directly from Client.

Beeline will not provide any third party: (i) direct, indirect, blanket, or unfettered access to Processed Data; (ii) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (iii) access to Processed Data if Beeline is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Beeline may provide Client's basic contact information to the third party.

I. Data Subject Rights; Assistance with Requests

Beeline will make available to Client, in a manner consistent with the functionality of the Platform and the Services and Beeline's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under Data Protection Requirements. If Beeline receives a request from a data subject to exercise one or more of its rights under Data Protection Requirements in connection with the Services for which Beeline is a data processor or Sub-processor, Beeline will promptly redirect the data subject to make its request directly to Client or its agents and where the data subject identifies Client in the data subject request, Beeline will also promptly notify the Client. Beeline will assist Client in fulfilling its obligations to respond to data subjects' requests by implementing technical and organizational measures set out here. Client will be responsible for responding to any such request and all communications with the data subject in accordance with Data Protection Requirements including, where necessary, by using the functionality of the Platform and the Services. Beeline shall comply with requests by Client to assist with Client's response to such a data subject request where Client is otherwise unable to leverage the functionality of the Platform and the Services as a result of Beeline's failure to make such functionality available.

J. Processing of Personal Data; GDPR

All Personal Data processed by Beeline in connection with providing the Services is obtained as part of either Client Data or data generated, derived or collected by Beeline or its Sub-processors, including data sent to Beeline as a result of Client's use of service-based capabilities. Data subjects and categories of Personal Data to be processed are as set out here. Pseudonymized identifiers may be included in data processed by Beeline in connection with providing the Services and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

1. Processor and Controller Roles and Responsibilities

Client and Beeline agree that Client is the controller of Personal Data and Beeline is the processor of such data, except: (a) when Client acts as a processor of Personal Data, in which case Beeline is a Sub-processor. When Beeline acts as the processor or Sub-processor of Personal Data, it will process Personal Data only on documented instructions from Client. Client agrees that its Agreements (including the DPA Terms and any applicable updates), are Client's complete documented instructions to Beeline for the processing of Personal Data. Any additional or alternate instructions must be agreed to by the parties according to the process for amending Client's Agreements. In any instance where the GDPR applies and Client is a processor, Client warrants to Beeline that Client's instructions, including appointment of Beeline as a processor or Sub-processor, have been authorized by the relevant controller.

2. Records of Processing Activities

To the extent the GDPR or any other Data Protection Requirements requires Beeline to collect and maintain records of certain information relating to Client, Client will, where requested, supply such information to Beeline and keep it accurate and up to date. Beeline may make any such information available to any supervisory or regulatory authority if required by the Data Protection Requirements.

K. Data Security

1. Security Practices and Policies

Beeline will implement and maintain appropriate technical and organizational measures to protect Client Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data transmitted, stored or otherwise processed. Those measures shall be set forth in a Beeline Security Policy. Beeline will make available to Client information reasonably requested by Client regarding Beeline security practices and policies subject to appropriate obligations of confidentiality.

2. Data Encryption

Client Data in transit over public networks between Client and Beeline, or between Beeline entities, is encrypted by default. Beeline also encrypts Client Data stored at rest.

3. Data Access

Beeline employs the principles of least privilege access mechanisms to control access to Client Data. Role-based access controls are employed to ensure that access to Client Data is for an appropriate purpose and approved with management oversight. Beeline maintains technical and organizational measures described here.

4. Client Responsibilities

Client is responsible for making an independent determination as to whether the technical and organizational measures for Services meet Client's requirements, including any of its security obligations under applicable Data Protection Requirements. Client acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Beeline provide a level of security appropriate to the risk with respect to its Personal Data. Client is responsible for implementing and maintaining privacy protections and security measures for components that Client provides or controls.

L. Auditing Compliance

Beeline will conduct audits of the security of the computers, computing environment, physical data centers, and cloud-services that it uses in processing Client Data as set forth in the Agreements.

M. Security Incident Notification

If Beeline becomes aware of a Security Incident regarding Client Data while processed by Beeline in the context of providing the Services, Beeline will promptly and without undue delay (1) notify Client of the Security Incident; (2) investigate the Security Incident and provide Client with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of security Incidents will be delivered to Client by any means Beeline selects, including via email. It is Client's sole responsibility to ensure Client maintains accurate contact information with Beeline for each applicable Service. Client is solely responsible for complying with its obligations under incident notification laws applicable to Client and fulfilling any third-party notification obligations related to any Security Incident.

Beeline shall reasonably assist Client in fulfilling Client's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

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

Client must notify Beeline promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Services at secincident@beeline.com.

N. Data Transfers

Client Data that Beeline processes on Client's behalf may not be transferred to or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Client appoints Beeline to transfer Client Data to the United States or any other country in which Beeline or its Sub-processors operate and to store and process Client Data, and Personal Data to provide the Services, except as described elsewhere in the DPA Terms.

Transfers from the EU will be made under the EU Adequacy Decision. Transfers from the UK (and Gibraltar) will be made under the UK Extension to the EU-U.S. DPF. Transfers from Switzerland will be made under the Swiss-U.S. DPF once in force. Where Beeline acts as a data processor, Beeline shall comply with its obligations under Article 28 of the GDPR for all such transfers. In the event that the EU-U.S. DPF ceases to be an approved method of data transfer, Beeline will select another approved method of data transfer. In the event that Beeline is unable to implement an alternative approved method of data transfer, Beeline shall promptly notify Client and Client may delete its affected Personal Data or terminate the affected Agreements for convenience in accordance with the terms therein.

All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

O. Data Retention and Deletion

At all times during the term of Client's Agreements, Client will have the ability to access, extract and delete Client Data stored in the Platform, subject to availability as set forth in the Agreements.

Beeline will return or destroy Client Data upon the expiration or termination of and in accordance with the terms of any Agreement, where such Client Data is no longer required to be processed, in accordance with Data Protection Requirements.

The Platform may not support retention or extraction of data by third-party software used or provided by Client and Beeline has no liability for the deletion of Client Data or Personal Data in this manner.

P. Notice and Controls on use of Sub-processors

Beeline may hire Sub-processors, including Beeline Affiliates, to provide certain limited or ancillary services on its behalf. Client authorizes Beeline's engagement of Sub-processors.

Where Beeline is acting as a data processor, Client hereby gives its general written authorization for the engagement of Beeline's Sub-processors. Beeline is responsible for its Sub-processors' compliance with Beeline's obligations in this DPA. Beeline's Sub-processors can be found here. When engaging any Sub-processor, Beeline will ensure via a written contract that the Sub-processor may access and use Client Data only to deliver the services Beeline has retained them to provide and is prohibited from using Client Data for any other purpose. Beeline will ensure that Sub-processors are bound by written agreements that provides for, in substance, the same data protection obligations as those binding Beeline under the Data Protection Requirements where applicable. Beeline agrees to oversee the Sub-processors to ensure that these contractual obligations are met.

From time to time, Beeline may engage new Sub-processors. Beeline will give Client notice (by updating this link or providing Client with a different mechanism to obtain notice of that update) of any new Sub-processor at least thirty (30) days in advance of engaging that new Sub-processor. If Beeline engages a new Sub-processor for a new Service that processes Client Data, Beeline will give Client notice prior to availability of that Service.

If Client does not reasonably approve of a new Sub-processor, then Client may terminate any subscription for the affected

Service for convenience without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. Client may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Beeline to re-evaluate any such new Sub-processor based on the applicable concerns.

Q. Limitation of liability

Except as regards towards data subjects and as otherwise provided by the Data Protection Requirements, either Party's liability to the other shall be as set forth in the applicable Agreements.

R. California Consumer Privacy Act (CCPA)

If Beeline is processing Personal Data within the scope of the CCPA, Beeline makes the following additional commitments to Client.

Beeline will process such Client Data on behalf of Client and Client is disclosing Client Data to Beeline for the limited purposes set forth and in accordance with these DPA Terms and Beeline shall not retain, use, or disclose that data for any purpose (including for any commercial purpose), outside of the direct business relationship between the parties and other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Beeline "sell" or "share" any such Client Data (as such are defined under the CCPA), to any third party for the purposes of cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

Beeline will comply with all applicable sections of the CCPA, including (with respect to the Client Data that it processes pursuant to the DPA Terms), providing a level of privacy protection no less secure than as set forth hereunder and as required by the CCPA. Beeline grants Client the right to take reasonable and appropriate steps to ensure that Beeline uses the Client Data that it processes pursuant to this DPA in a manner consistent with Client's obligations under the CCPA as set forth under and in accordance with the DPA Terms.

Client may take reasonable and appropriate steps to stop and remediate Beeline's unauthorized use of Client Data by removing or by requesting the removal of such Client Data from Beeline's Platform. Upon receipt of such written notice, Beeline will promptly, and not later than 30 days from its receipt of such notice, assist Client with such removal. Client acknowledges and agrees that such removal of Client Data from the Beeline Platform shall not constitute a termination for breach by Beeline.

Beeline shall enable Client to comply with consumer requests made pursuant to the CCPA as set forth under **Section I (Data Subject Rights; Assistance with Requests)** above and shall contract with its Sub-processors in compliance with the CCPA as set forth under **Section P (Notice and Controls on use of Sub-processors)** above.

Beeline will notify Client where it reasonably determines that it cannot meet its obligations under the CCPA. These CCPA terms do not limit or reduce any data protection commitments Beeline makes to Client in the DPA Terms or other Agreements between Beeline and Client.

S. How to Contact Beeline

If Client has any questions, please contact Beeline at the following mailing address:

Attn. Legal Email: legal@beeline.com