Data Processing Addendum

This Data Processing Addendum ("**DPA")** is incorporated into, and is subject to the terms and conditions of, the Agreement between Paycor, Inc. ("Processor") and Client ("Controller") for the purchase of all services from Processor, except for Paycor Smart Sourcing, (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as "Services") (the "Agreement") to reflect the parties' agreement regarding the Processing of Personal Data.

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. DEFINITIONS

1.1. "Authorized Subcontractor" means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Client Personal Information to enable Processor to perform its obligations under this Addendum or the Agreement and who is either (1) listed at https://knowledge.paycor.com/resources/paycor-subprocessors-and-data-privacy at the time the parties enter into this Addendum or (2) later authorized by Controller, pursuant to Section 3.3 of this Addendum.

1.2. "CCPA" or "CCPA, as amended" means the California Consumer Privacy Act of 2018, Cal. Civ. Code ss1798.100 et. Seq., and its implementing regulations, as amended by the CPRA.

1.3. "CPRA" means the California Privacy Rights Act of 2020, and its implementing regulations.

1.4. "Personal Data" means any nonpublic Client Data maintained by Client and processed by Paycor solely on Client's behalf that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or natural person, to the extent that such information is protected as "personal information" (or analogous variation of such term) under applicable U.S. Data Protection Laws.

1.5. "Process" or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.6. "U.S. Data Protections Laws" means the various applicable data protection and privacy laws of the state(s), which may include but are not limited to, California ("CCPA", "CPRA"), Colorado (Colorado Privacy Act of 2021 "CPA") and Virginia (Virginia Consumer Data Protection Act of 2021 "VCDPA").

1.7. The terms, "Controller", "Processor", "Sell", and "Share" shall have the same meanings given under applicable U.S. Data Protection Laws.

2. PROCESSING OF DATA

2.1. The Parties acknowledge that with regard to the Processing of Personal Data performed solely on behalf of Client, (i) Client is the Controller, and (ii) Paycor is the Processor.

2.2. Client, in its use of the Services, and Client's directions issued to Processor, including those directing the Processing of Personal Data ("Instructions"), shall comply with applicable U.S. Data Protection Laws. Client shall establish and maintain all required legal bases to (i) collect, Process, and transfer Personal Data to Processor, and (ii) authorize Processor's Processing/Processing activities on Client's behalf.

2.3. Processor shall Process Personal Data, except for provided below, only (i) for the purposes set forth in the Agreement, (ii) in accordance with the terms and conditions of the Agreement and any other documented Instructions provided by Controller, and (iii) in compliance with U.S. Data Protection Laws. Personal Data shall be Processed for the purpose of supporting the Services.

2.4. Processor shall, in a timely manner, securely delete or destroy, all Personal Data after termination of the Agreement; except such Personal Data that cannot be deleted or destroyed pursuant to a statutory obligation or related legal matter (e.g. maintenance of a litigation hold, storage of documents for the duration of a statute of limitations, etc.), which shall then remain protected by the DPA.

2.5. **CCPA.** This subsection shall apply with regards to the Processing of Personal Data of California residents, as subject to the CCPA, as amended.

- 2.5.1 For the purposes of this section, the terms "Business", "Business Purpose", and "Service Provider" shall have the meanings as set forth in the CCPA, as amended. The Parties acknowledge that for the purposes of the CCPA, the Client is the "Business" and Paycor is the "Service Provider" (to the extent that such terms apply).
- 2.5.2 Service Provider shall Process Personal Data only: (i) for limited Business Purposes as contemplated by the Agreement, (ii) in compliance with its obligations under the CCPA, as amended, and (iii) subject to the reasonable security procedures and practices as detailed in Section 5.
- 2.5.3 Service Provider shall not: (i) sell or share Personal Data, (ii) retain, use, or disclose Personal Data for any purpose other than for the Business Purposes specified in the contract, including retaining, using, or disclosing the Personal Data for a commercial purpose other than the Business Purposes specified in this agreement, or as otherwise permitted by the CCPA, as amended, (iii) retain, use, or disclose the information outside of the direct business relationship between the Business and Service Provider, or (iv) combine the Personal Data that the Client receives pursuant to this agreement with Personal Data that it receives from or on behalf of another person or persons, or collects from its own interaction with the individuals except where authorized under the CCPA, as amended.
- 2.5.4 Business shall promptly notify Service Provider if it reasonably believes that unauthorized access has occurred to Personal Data transferred under the Agreement and shall allow Service Provider a reasonable opportunity to remedy the unauthorized access.
- 2.5.5 Service Provider will notify Business if it makes a determination that it can no longer meet its obligations under the CCPA, as amended.

3. ACCESS BY AUTHORIZED PARTIES

3.1. **Authorized Employees.** Processor shall take commercially reasonable steps to ensure the reliability and appropriate training of any employee of Processor who has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement ("Authorized Employee").

3.2. Processor shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Processor, any Personal Data except in accordance with their obligations in connection with the Services.

3.3. **Authorized Subcontractors.** Controller acknowledges that Processor may (i) engage the Authorized Subcontractors to access and Process Personal Data in connection with the Services and (ii) from time to time, engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data. A list of Processor's current Authorized Subcontractors (the "List") is available at https://knowledge.paycor.com/resources/paycor-subprocessors-and-data-privacy (such URL may be updated by Processor from time to time).

3.4. Processor, or any entity that directly or indirectly controls, is controlled by, or is under common control with, the Processor, has entered into a written agreement with each Subcontractor containing appropriate safeguards for the protection of Personal Data. Where Processor engages a new Subcontractor for Processing on behalf of the Controller, the same or materially same data protection obligations as set out in this DPA, shall be imposed on such new Subcontractors.,

4. SECURITY OF PERSONAL DATA

4.1. Processor shall maintain commercially reasonable administrative, physical, and technical measures that are designed to protect the security, confidentiality, and integrity of Personal Data, and that are reasonably appropriate to the risks represented by the processing and nature of the provided Personal Data to be protected and designed to guard against the accidental or unauthorized access, use, loss, or disclosure of Personal Data while it is in the Paycor product. Controller acknowledges an independent duty to comply with any and all U.S. Data Protection Laws in connection with its provision of Personal Data to Processor. Controller may not perform any security penetration tests or security assessment activities without the express advance written consent of Processor.

4.1.1. Controller acknowledges and accepts that to safeguard Personal Data, upon any indication of breach of security, Processor may immediately suspend any or all of Controller's, and its Authorized Individuals', use of the Services, which utilize an internet connection, without prior notice.

4.1.2. Any credentials (including, but not limited to: usernames, passwords, and security questions and answers) that can be used to access the Processor's Services and/or Products ("Paycor Credentials") are proprietary and confidential. Individuals with Paycor Credentials ("Users") may not disclose Paycor Credentials, authorize any other person to use their Paycor Credentials, or otherwise grant access to Processor's Services. To protect Paycor Credentials and the proprietary and confidential information that can be accessed by using them, Processor may disable a User's Paycor Credentials if it reasonably determines that such Credentials are being used by more than one person. Controller agrees to require Users to: use reasonable efforts maintain the privacy and security of Paycor Credentials and exit from User's Paycor account at the end of each session.

4.1.3. Processor shall not be liable for any damages Controller, a third party, or any User may incur resulting from a failure to comply with this section or as a result of someone else using Users' credentials or access provided by such credentials, either with or without the applicable Users' knowledge.

4.2. Processor agrees to treat all Personal Data that Controller discloses to Processor in accordance with applicable privacy laws, rules, and regulations. In the event that Processor becomes aware that sensitive Personal Data of any of Controller's employees has been intentionally disclosed to or acquired by unauthorized parties (any such incident a "Data Breach"), Processor will, to the extent required by U.S. Data Protection Laws, promptly notify Client of such disclosure or acquisition.

4.2.1. Controller agrees that Processor may disclose Personal Data to: (i) Processor's employees or agents (including its attorneys, auditors, or accountants) in the ordinary course of its business; (ii) non-affiliated third parties who need access in order for Processor to carry out the Services or any other services requested by Controller, including but not limited Third-Party Providers; (iii) employees, agents, affiliates, or contractors of Controller that supplied such Personal Data to Processor or that Controller has authorized to receive such Personal Data from Processor; or (iv) as is otherwise required by Applicable Law (including but not limited to responding to subpoenas and investigations by government regulatory authorities). Processor shall take appropriate measures to maintain the security and confidentiality of Personal Data, treating such information in a manner similar to which Processor treats its own information.

5. RIGHTS OF DATA SUBJECTS

5.1. Processor shall, to the extent legally permitted, refer an identified or identifiable individual to whom Personal Data relates ("Data Subject" or "Consumer"), to Controller, if Processor receives a request from a Data Subject or Consumer to exercise their privacy rights (to the extent available to them under applicable U.S. Data Protection Laws). Controller will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.

6. CROSS-BORDER DATA TRANSFERS

6.1 If at any time Controller requires the processing of Personal Data by Processor which includes transfers (either directly or via onward transfer) from the European Economic Area *(*EEA), Switzerland and/or the UK, Controller must obtain a DPA for international transfers by emailing privacy@paycor.com before such processing can begin. Client understands and acknowledges that the Paycor HR AnswerLink service is supported by a third party that does not adhere to GDPR compliance requirements.

7. LIMITATION OF LIABILITY

7.1. The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.

Last Updated: October 2024