An executable version of this document can be found here.

Paylocity Data Protection Addendum

This Paylocity Data Protection Addendum ("DPA") supplements and forms part of the Subscription Services Agreement ("Agreement") entered into by Client and Paylocity Corporation or any of its Affiliates (each, "Paylocity"), on behalf of itself and/or, where applicable, the Affiliate executing the Agreement, each a "Party" and collectively the "Parties."

This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Agreement or under Applicable Data Protection Laws with cognate terms construed accordingly. This DPA is effective on the Effective Date of the Agreement.

1. Definitions

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, whereas "control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**Applicable Data Protection Laws**" means any applicable law, rule, regulation, decree, order, or regulatory guidance relating to the Processing of Client Personal Information under the Agreement, including for data security, data protection and/or privacy, in any jurisdiction.

1.3. "**Client Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household that Client provides or discloses to Paylocity or that Paylocity otherwise collects, stores, or otherwise Processes on behalf of Client in connection with the Agreement.

1.4. "**Controller**" means the entity which determines the purpose and means of the Processing of Client Personal Information.

1.5. "**Data Subject**" means an identified or identifiable person to whom Client Personal Information relates.

1.6. "**Data Subject Request**" means a request from a Data Subject seeking to exercise their rights under Applicable Data Protection Laws.

1.7. **"EEA"** means the European Economic Area.

1.8. **"GDPR"** means the EU General Data Protection Regulation 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).

1.9. **"Permitted Affiliate"** means any of Client's Affiliates that (i) are permitted to use the Services pursuant to the Agreement, but have not signed their own separate agreement with us, (ii) qualify as a Controller of Client Personal Information Processed by Paylocity, and (iii) are subject to Applicable Data Protection Laws.

1.10. "**Personal Data Breach**" means any confirmed accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or acquisition of, or access to, Client Personal Information under Paylocity's control.

1.11. **"Process"** or **"Processing"** means any operation performed on Client Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.12. **"Processor**" means an entity which Processes Client Personal Information on Controller's behalf.

1.13. "**Restricted Transfer**" means a transfer (directly or via onward transfer) of Client Personal Information that is subject to an Applicable Data Protection Law to a country outside of such applicable country that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable).

1.1.1 **"Services**" means the services and other activities to be supplied or carried out by or on behalf of Paylocity for Client pursuant to the Agreement.

1.14. **"Standard Contractual Clauses"** means the annex to the standard contractual clauses, also known as "SCCs," or "EU SCCs" attached to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council found at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

1.15. "**Sub-processor**" means any Processor (excluding an employee of Paylocity or any of its subcontractors) engaged by and/or appointed by or on behalf of Paylocity to assist in fulfilling its obligations to Process Client Personal Information on behalf of Client in connection with the Agreement.

1.16. **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, found at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

2. Processing of Client Personal Information

2.1 **Roles of the Parties.** The Parties shall comply with Applicable Data Protection Laws in the Processing of Client Personal Information. The Parties agree that, with respect to all Client Personal Information and purposes of Processing described in Annex 1, Client is the Controller, or a Processor acting on behalf of a Controller, and controls the purposes and means of Processing Client Personal Information, and Paylocity is the Processor and Processes all such Client Personal Information on behalf of Client.

2.2 **Client Responsibilities**. Client shall be responsible for determining whether the Services are appropriate for the storage and processing of Client Personal Information under Applicable Data Protection Laws. Client further agrees that:

2.2.1 it will comply with its obligations under Applicable Data Protection Laws and its contractual obligations with Paylocity regarding its use of the Services and the processing of Client Personal Information;

2.2.2 it is solely responsible for the accuracy, quality, and legality of Client Personal Information including the means by which such information was collected;

2.2.3 it has provided notice and obtained all consents, permissions and rights necessary for Paylocity and its Sub-processors to lawfully Process Client Personal Information for the purposes contemplated by the Agreement (including this DPA); and

2.2.4 it will notify Paylocity if it is unable to comply with its obligations described above or if its processing instructions will cause Paylocity or its Sub-processors to be in breach of Applicable Data Protection Laws. For the avoidance of doubt, Paylocity shall not be responsible for compliance with any laws that are only specific to Client or Client's industry and are not generally applicable to Paylocity in its capacity as a service provider.

2.3 **Paylocity Responsibilities**. Paylocity shall:

2.3.1 only Process Client Personal Information pursuant to Client's instructions and as described in Annex 1 hereto;

2.3.2 not sell or share any Client Personal Information except to the extent required by Applicable Data Protection Laws or as permitted by the Agreement in connection with a merger, acquisition, change of control, or sale of all or substantially all of the assets to which the Agreement relates;

2.3.3 not retain, use, or disclose Client Personal Information outside of the direct business relationship between the Parties or for any purpose other than the purpose of performing the Services specified in the Agreement, which shall include (i) providing the Services under the Agreement; (ii) verifying or maintaining the quality or safety of the Services, and to improve, upgrade or enhance the Services; and (iii) complying with Paylocity's legal obligations;

2.3.4 not combine Client Personal Information with other information received from third parties except as required for the fulfillment of the Services; and

2.3.5 promptly notify Client in writing, unless otherwise prohibited under Applicable Data Protection Laws, if Paylocity:

2.3.5.1 reasonably determines that any instructions from Client conflict with, infringe, or violate the requirements of Applicable Data Protection Laws;

2.3.5.2 reasonably determines that it can no longer meet its obligations under Applicable Data Protection Laws; or

2.3.5.3 receives any complaint, notice, or communication that directly or indirectly relates to either Party's compliance with Applicable Data Protection Laws in connection with Processing associated with the Services.

3. Paylocity Personnel

Paylocity shall take reasonable steps such that any of Paylocity's personnel or any Sub-processors who may have access to Client Personal Information have a need to know the relevant Client Personal Information and are under an appropriate obligation of confidentiality.

4. Security

Paylocity shall, in relation to Client Personal Information, implement appropriate technical and organizational measures to attain a level of appropriate security, as set forth in Annex 2 of this DPA.

5. Sub-processing

5.1 Client authorizes Paylocity to engage the Sub-processors found in Annex 3 of this DPA, to Process Client Personal Information as required to provide the Services under the Agreement.

5.2 Upon reasonable request, Paylocity shall provide to Client additional information related to its Sub-processors.

5.3 Where required by Applicable Data Protection Laws, Paylocity shall notify Client of any Sub-processor that Paylocity proposes to engage through updates to the Sub-processors notification mechanism outlined in Annex 3, and respond in good faith to any reasonable objections by Client.

5.3.1 Client may, in good faith, object to Paylocity's use of a new Sub-processor by notifying Paylocity (email notifications shall be acceptable) within thirty (30) days of Paylocity's notice to Client and such notice to Paylocity shall explain the reasonable grounds for objection.

5.3.2 If Client timely objects to a new Sub-processor, Paylocity will use commercially reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Client Personal Information by the objected-to new Sub-processor.

5.4 If the Parties are unable to resolve such objection or Paylocity is unable to resolve or make available such change within a reasonable period of time, Client may terminate the Agreement with respect to those Services which cannot be provided by Paylocity without the use of the objected-to new Sub-processor by providing written notice to Paylocity. If it is not possible to partially terminate the Agreement, Client may terminate the Agreement in whole, subject to the terms of the Agreement.

5.5 Paylocity shall carry out adequate due diligence to assure that its Sub-processors are capable of providing the level of protection for Client Personal Information required by the Agreement.

5.6 Paylocity shall remain liable for the actions and omissions of its Sub-processors.

5.7 Paylocity shall enter into a written contract with each Sub-processor that complies with Applicable Data Protection Laws and includes terms which offer at least the same level of protection for Client Personal Information as those set out in this DPA.

5.8 Where Client elects to integrate the Services with other third-party services, which may allow for the transfer of Client Personal Information to such third parties, Client acknowledges and agrees that (a) such third parties shall not be considered Sub-processors for the purpose of this section; (b) such transfers are conducted on Client's instruction; (c) Client shall be solely responsible for ensuring that it has the appropriate agreements in place with such third parties in respect of the Processing of any transferred Client Personal Information (which Paylocity is not a party to); and (d) Client shall be solely responsible for such transfers and any related compliance with Applicable Data Protection Laws.

6. Data Subject Request

6.1 Paylocity shall, to the extent legally permitted, notify Client without undue delay of any request it receives from a Data Subject regarding their rights under Applicable Data Protection Laws. Paylocity shall not respond to Data Subject Requests itself, and Client shall be solely responsible for handling such requests.

6.2 Paylocity shall assist Client in fulfilling its obligations to respond to Data Subject Requests under Applicable Data Protection Laws. Paylocity shall promptly comply with any instruction from Client requiring Paylocity to provide, amend, transfer, or delete Client Personal Information, unless any such instruction violates or would cause Paylocity to violate Applicable Data Protection Laws, in which case Paylocity will promptly inform Client in writing.

7. Personal Data Breach

7.1 Paylocity shall notify Client in writing (which may be by email) without undue delay upon Paylocity becoming aware of a Personal Data Breach impacting Client Personal Information, and shall provide Client with sufficient information to allow Client to evaluate its obligations under Applicable Data Protection Laws to notify Data Subjects, regulatory authorities or other parties of the Client Personal Information Breach. Paylocity shall reasonably cooperate with Client and take commercially reasonable steps to investigate, mitigate, and remediate such Personal Data Breach.

7.2 Paylocity shall not make any notification to regulatory authorities or Client's Data Subjects unless Client has given Paylocity prior express written permission or such notification is required by Applicable Data Protection Laws.

7.3 Except where otherwise required under Applicable Data Protection Laws, Client shall be solely responsible for determining whether Client will (a) provide notice of the Personal Data Breach affecting Client Personal Information to any Data Subjects, regulators, law enforcement agencies or others, and the contents and delivery method of the notice; and (b) offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

8. Data Protection Impact Assessment and Prior Consultation

Paylocity shall, in a commercially reasonable manner, assist Client in meeting its obligations in relation to data protection impact assessments and prior consultations with regulatory bodies by cooperating with reasonable requests from Client for information about its Processing activities and data protection practices, taking into account the nature of Processing and the information available.

9. Deletion or Return of Client Personal Information

9.1 Until the effective date of the expiration or termination of the Subscription Term, Client shall have the ability to retrieve Client Personal Information. After the effective date of the expiration or termination of the Subscription Term, Client may retrieve any remaining Client Personal Information, subject to the terms and conditions set out in the Agreement.

9.2 After termination or expiration, Paylocity shall, and shall cause its Sub-processors to, securely delete or anonymize (in accordance with standards prescribed under Applicable Data Protection Laws) Client Personal Information in the ordinary course of business when no longer necessary to perform services under the Agreement and in accordance with Paylocity's retention policies.

9.3 After the termination or expiration of Services and before the retention period is concluded, Client may request deletion of Client Personal Information. Paylocity shall delete or anonymize existing copies of Client Personal Information unless retention is required by Applicable Data Protection Laws (or other laws governing the Processing of such data) and only to the extent and for such period as required by applicable laws.

9.3.1 Client acknowledges that when Client requests deletion of Client Personal Information by Paylocity, the deleted Client Personal Information will no longer be retrievable or accessible following its deletion, and any of Paylocity's obligations to such Client Personal Information ends upon deletion.

9.4 Where Client Personal Information is retained after termination or expiration, Paylocity shall keep such Client Personal Information confidential and shall Process such Client Personal Information only as necessary for the purpose(s) specified in the Agreement and in accordance with Applicable Data Protection Laws requiring its storage and for no other purpose.

9.5 Notwithstanding anything to the contrary in this Section, the obligations set forth herein shall not apply to the extent that the Client Personal Information, or any data derived therefrom, has been deidentified, anonymized, or aggregated by Paylocity in a manner that it no longer constitutes Client Personal Information under Applicable Data Protection Laws.

10. Audit Rights

Paylocity shall reasonably cooperate with Client's efforts to verify Paylocity's compliance with this DPA, which efforts may include periodic audits (not to exceed one (1) audit in any twelve (12) month period), conducted at Client's expense by Client (or a qualified, independent third-party auditor on Client's behalf) as described in this Section 10. Client and Paylocity shall mutually agree to the dates, times, and scope of any audit of Paylocity, provided that this requirement shall not oblige Paylocity to provide access to information concerning: (i) information relating to Paylocity's other clients; (ii) Paylocity's non-public external reports; or (iii) Paylocity's proprietary information. Client or Client's auditor shall not damage Paylocity's equipment, injure Paylocity's personnel, or disrupt Paylocity's business in the course of such an audit. Notwithstanding the foregoing, Client shall be entitled to conduct

more than one audit in any twelve (12) month period in the event of a Personal Data Breach or a request from a regulatory body.

11. International Data Transfers

11.1 General Obligations. Paylocity will only transfer Client Personal Information across international borders and between jurisdictions to the extent permitted by this Section 11 and in accordance with Applicable Data Protection Laws.

11.2 Data transfers from the EU/EEA, UK, and Switzerland to the United States. For such transfers, Paylocity participates in and certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (together, the "Data Privacy Framework"). As required by the Data Privacy Framework, Paylocity will (i) provide at least the same level of privacy protection as is required by the Data Privacy Framework Principles; (ii) notify Client if Paylocity makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, take reasonable and appropriate steps to remediate unauthorized Processing.

11.3 Data Transfers from the EU/EEA, UK, and Switzerland to a country other than the United States. For such transfers, the Parties agree that when the transfer of Client Personal Information from Client (as "Data Exporter") to Paylocity (as "Data Importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the Restricted Transfer will be made in accordance with Applicable Data Protection Laws and, if applicable, subject to the Standard Contractual Clauses ("SCCs"), which are deemed incorporated into and form a part of this DPA, as follows:

(a) EU/EEA Personal Information

11.3.1 Transfers of Client Personal Information of EU Data Subjects from Client (Data Exporter) in the EU/EEA to Paylocity (Data Importer) outside the EU/EEA will be conducted in accordance with this DPA and the provisions contained in module 2 (controller-to-processor) of the EU SCCs.

11.3.2 Where the transfer of Client Personal Information is subject to the GDPR and the transfer relies on the EU SCCs, then the following amendments shall apply to the EU SCCs: (i) for the purposes of Section I, Clause 7, the optional docking clause applies; (ii) in Clause 9, Option 2 applies and changes to Sub-processors will be notified in accordance with the 'Sub-processors' section of this DPA; (iii) in Clause 11, Data Subjects shall also be able to lodge a complaint with an independent dispute resolution body; (iv) in Clause 17, option 1 shall apply and the Parties agree that the clauses shall be governed by the law of the Czech Republic; (v) in Clause 18(b) the Parties choose the courts of the Czech Republic as their choice of forum and jurisdiction; (vi) the Annexes of the EU SCCs will be deemed completed with the information set out in the Annexes of this DPA; (vii) the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR; and (viii) if and to the extent the EU SCCs conflict with any provision of this DPA, the EU SCCs will prevail to the extent of such conflict.

11.3.3 Where transfers of Client Personal Information of EU/EEA Data Subjects are conducted by Client (Data Importer) on behalf of their client (Controller), module 3 (processor-to-processor) of the EU SCCs is applicable to such transfers, and the following terms shall apply in addition to those in section 11.3.2:

11.3.3.1 For the purposes of Clause 8.1(a), (b) and (c), Client hereby informs Paylocity that it acts as Processor under the instructions of the relevant Controller with respect to Client Personal Information. Client warrants that its Processing instructions as set out in the Agreement, including this DPA and its authorizations to Paylocity for the appointment of Sub-processors in accordance with this DPA, have been authorized

by the relevant Controller. Client is solely responsible for conveying any Sub-processor notifications to the relevant Controller where appropriate.

11.3.3.2 For the purposes of Clause 8.6(c) and (d), Paylocity shall provide notification of a Personal Data Breach to Client in accordance with this DPA.

11.3.3.3 For the purposes of Clause 8.9, all enquiries from the relevant Controller shall be handled solely by Client. If Paylocity receives an enquiry directly from a Controller, it shall forward the enquiry to Client and Client shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.

11.3.3.4 For the purposes of Clause 10 and subject to this DPA, Paylocity shall notify Client about any request it has received directly from a Data Subject without obligation to handle it and is not obligated to notify the relevant Controller. Client shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.

(b) UK Personal Information

11.3.4 *Controller-Processor Transfers*. Transfers of Client Personal Information of UK Data Subjects from Client (Data Exporter) in the UK to Paylocity (Data Importer) outside the UK will be conducted in accordance with this DPA and UK Addendum

11.3.5 *IDTA Additional Terms*. Where the transfer of Client Personal Information is subject to the UK GDPR and the transfer relies on the International Data Transfer Addendum to the EU SCCs, the EU SCCs will apply in accordance with sub-section (a) and the following modifications: (i) the EU SCCs will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "Importer"; and (iii) any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) Swiss Personal Information

11.3.6 In relation to Client Personal Information subject to the Swiss Federal Act on Data Protection (FADP), the EU SCCs will apply in accordance with sub-section (a) and the following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " (FDPIC) and the "relevant courts in Switzerland".

12. General Terms

12.1 Order of Precedence. For data transfers from the EU/EEA, UK, and Switzerland to a country other than the United States, in the event of any conflict or inconsistency between this DPA and the EU SCCs (or, where applicable, the UK or Swiss equivalent), the EU SCCs (or the UK or Swiss equivalent) shall prevail. In the event of inconsistencies between the provisions of this DPA and the Agreement, or any other agreements between the Parties, the provisions of this DPA shall prevail with respect to the subject matter hereof.

12.2 Severability. 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(s) 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.

12.3 Authorization. Client represents and warrants on an ongoing basis that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, its Permitted Affiliate. Client (not including Permitted Affiliate) is responsible for exercising any rights, seeking any remedy, providing all instructions, authorizations and other communications to Paylocity in a combined manner for all relevant Affiliates, and receiving any communications from Paylocity, related to this DPA on behalf of Client's Permitted Affiliate.

12.4 Third-Party Beneficiaries. Except as required by Applicable Data Protection Laws, there are no third-party beneficiaries of this DPA, including but not limited to Client's Permitted Affiliate.

ANNEX 1 – Details of Processing

A. List of Parties

Data Exporter:
Name: Client, as identified in the Agreement (on behalf of itself and Permitted Affiliates).
Address: Client's address, as set out in the applicable Order Form.
Contact person's name, position, and contact details: Client's contact details as set out in the Order Form and/or as set out in Client's Paylocity account.
Activities relevant to the data transferred under these Clauses: Processing of Client Personal Information in connection with Client's use of the Services under the Agreement.
Role (Controller/Processor): Controller (either as the Controller; or a Processor acting on behalf of another Controller)

Data Importer:
Name: Paylocity Corporation
Address: 1400 American Lane, Schaumburg, IL 60173
Contact person's name, position and contact details: Corinne Tirone, Senior Director, Privacy and Compliance, privacy@paylocity.com
Activities relevant to the data transferred under these Clauses: Processing of Client Personal Information in connection with Client's use of the Services under the Agreement.
Role (Controller/Processor): Processor

B. Description of Transfer

Categories of Data Subjects whose personal data is transferred
- employees of Client and employees of Clients' clients, where applicable (personnel engaged by Data Exporter or its clients, where applicable)
- contractors (individuals acting in a business capacity as independent contractors to Data Exporter)
- job applicants (individuals seeking employment from Data Exporter)
- other (e.g., dependents, beneficiaries)

Categories of personal data transferred
- personal identification (name, date of birth)
- contact details (email, phone, address)
- real-time or precise location
- education and training details
- employment-related data
- family, lifestyle, and social circumstances
- financial, economic and insurance data, including financial account numbers
- billing and payment information
- digital, device and social media identifiers or digital profiles
- account credentials
- contents of communications not directed to Data Exporter
- any other categories of Client Personal Information provided by Data Exporter in connection with the Services.

Sensitive Data transferred and applied restrictions or safeguards
- Financial information (bank account information, bank account number, bank statements, credit card number, debit card number, direct deposit information, routing number, credit history, state withholding tax information)
- Racial or ethnic origin
- Nationality
- Citizenship status
- Driving license number

- Government identifiers (Social Security Number, passport numbers, national identification number, national identity card details)
- Data concerning health
- Biometrics data (retina scan, facial recognition, voice recognition, sleep pattern recognition)
- Disability information (disability description, disability or specific condition linked to an ADA)
- Genetic data (genetic sequence)
- Geolocation information
- Political affiliation and activities
- Religion/religious beliefs
- Trade union membership
- Sexual orientation
- Sensory and electronic information

Frequency of the transfer
Continuous

Nature of the Processing
Client Personal Information will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:
1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to Client; and/or
2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by Applicable Data Protection Laws and other applicable laws.

Purpose of the transfer and further Processing
As necessary to provide the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Client in its use of the Services.

Period for which personal data will be retained
Subject to the 'Deletion or Return of Client Personal Information' section of this DPA, Paylocity will Process Client Personal Information for the duration of the Agreement, unless otherwise agreed in writing.

For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing
Transfers to Sub-processors comprise the same categories of Data Subjects and Client Personal Information, and duration as set out above. The Sub-processors provide services to Data Importer in connection with its delivery of Services.

Competent supervisory authority/ies in accordance with Clause 13 of the SCCs
- For transfers from the European Economic Area: Czech Republic's Office for Personal Data Protection
- For transfers from the UK: UK Information Commissioner's Office
- For transfers from Switzerland: Swiss Federal Data Protection and Information Commissioner (FDPIC)

ANNEX 2 – Security Measures

Paylocity security measures are described in this Annex 2. The Security Program is supported by documented policies and standards that are reviewed at least annually. To promote transparency and provide assurance, Paylocity makes copies of its current security certifications, reports, and related documentation available to clients through the applicable Trust Center (https://www.paylocity.com/who-we-are/protecting-our-clients/).

These safeguards are designed to align with applicable laws and regulations and include the following measures:

Organizational Security Measures	**Security Roles & Responsibilities.** Information security oversight is the responsibility of the Paylocity Chief Information Security Officer (CISO), who has established an operating model consisting of multiple teams with subject matter disciplines designed to achieve the objectives of the Security Program. **Disaster Recovery; Business Continuity.** Paylocity maintains business continuity procedures (including disaster recovery and crisis management protocols) and tests them at least annually, as appropriate to the size, nature, and complexity of its operations. **PCI DSS Obligation.** To the extent the Spend Management Services (as defined in the Agreement) are in scope, Paylocity ensures the security of cardholder data it possesses or otherwise stores, processes, or transmits on behalf of the Client, or to the extent that it could impact the security of the Client's cardholder data environment.
Administrative Security Measures	**Personnel and Training.** Paylocity provides relevant data privacy and security training at a minimum annually and requires personnel with access to Client Data to abide by Paylocity confidentiality and security obligations. **Third-Party Access.** Paylocity conducts appropriate due diligence on third parties involved in performing the Services or who have access to systems that contain Client Data.
Technical Security Measures.	**Physical Security.** Paylocity maintains physical and environmental security measures that control and restrict physical access to, and provide environmental protection for, systems that contain Client Data. **Security and Vulnerability Scanning and Patch Management.** Paylocity maintains a formal patch management program and performs patch management activities on relevant systems that process Client Data. **Application Security Tests and Assessments.** At a minimum annually, Paylocity performs a security assessment on relevant systems that handle, maintain, or process Client Data. **Network Security.** Paylocity deploys appropriate network security and information transfer controls designed to protect Client Data, including the use of firewalls, intrusion detection and prevention systems, proxy servers and secure file transfer technologies, or relevant equivalent technologies, in the operation of systems and facilities, in each case, consistent with industry standard. **Security Event Logs.** Paylocity logs access to the systems used to host Client Data and/or provide the Services to the Client for compliance, audit, and incident investigation purposes. **Access and Authorization.** For accounts created, administered, and operated by Paylocity, Paylocity implements appropriate access controls and employs commercially reasonable physical, administrative, and technological access control mechanisms designed to prevent unauthorized access to Paylocity facilities and systems that store or allow access to Client Data.
Data Transmission and Storage	**Data Encryption.** Paylocity utilizes cryptographically secure protocols that are consistent with commercially reasonable standards to encrypt Client Data when in transit and at rest or transported/stored via physical media (e.g., tapes, disks, etc.)

ANNEX 3 – Sub-processors

Paylocity engages Sub-processors to Process Client Personal Information as necessary to provide the Services under the Agreement. A list of Sub-processors is available at the following links:

- *For Blue Marble Payroll, LLC:* Blue Marble Payroll List of Sub-processors
- *For Paylocity Corporation and its other Affiliates:* Paylocity Corporation List of Sub-processors

To ensure timely updates regarding any changes to the Sub-processors list, Client agrees to subscribe to the notification mechanisms available at the links by clicking the bell icon located at the top right corner of the relevant page.