



HOW TO EXECUTE THIS DATA PROCESSING ADDENDUM

To execute this Addendum, Client must:

1. complete the information in the signature box on page 7 and sign;
2. complete the data exporter information on page 20; and
3. send the completed and signed Addendum to Pegasystems at CommOps@pega.com. Upon Pegasystems' receipt of the validly signed Addendum, this Addendum will be legally binding.

DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**Addendum**") applies to an agreement signed by both parties for Client to receive Subscription Services, Software, or purchase Professional Services (each, a "**Schedule**"), between the Pegasystems corporate entity ("**Pegasystems**") and the client that appears on the signature page below ("**Client**") that are parties to such Schedule, pursuant to which Pegasystems processes Client Personal Data. This Addendum only applies to direct sales between Pegasystems and Client. By following the below instructions to execute this Addendum, Client agrees to the terms herein on behalf of itself, and on behalf of Client's affiliates to the extent they access Professional Services or Subscription Services provided by Pegasystems under a Schedule. For the avoidance of doubt, signature of the Addendum on page 7 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including its annexes; and where applicable of the Model clauses referenced herein.

This Addendum is between Pegasystems and Client (each a "**party**" and together the "**parties**") and is made part of the Schedule(s) in effect between the parties.

For the purposes of this Addendum, the following definitions apply:

"Affiliates" are those entities that control, are controlled by, or are under common control with a party to the Agreement. Affiliates may be entitled, subject to the terms of this Agreement and the applicable Schedule, to use the Subscription Services, Software, or purchase maintenance services or Professional Services. For any Schedule to which an Affiliate is a party, the Affiliate will be additionally considered the Client for purposes of the Agreement and such Schedule.

"Adequate Countries" mean (a) countries in the European Economic Area ("**EEA**") and (b) countries formally recognized by the European Commission as providing an adequate level of data protection.

"Business Contact Data" means business contact information (the names, titles and roles, business phone and facsimile numbers, business office and email addresses) of Client's or Pegasystems' employees and contractors.

"CCPA" means the California Consumer Privacy Act, as amended, and any successor legislation.

"Client Application" means a unique collection of rules and processes as part of one or more new RuleSets that are created using the Software and that provide specific business functionality for the Client.

"Client Data" means any information received from or on behalf of Client that is stored, transferred, or processed by the Subscription Services.

"Client Personal Data" means any information relating to any identified or identifiable natural person, or any other data regulated by Data Protection Law, that is transferred, processed, or stored as part of the Subscription Services by or on behalf of Client.

"Data Protection Law" means, to the extent governing the processing of Client Personal Data under the applicable Schedule(s) to which Client or Pegasystems is subject, any of the following: (i) all applicable data protection and privacy legislation, regulations and guidance in the European Economic Area, the United Kingdom and Switzerland including the General Data Protection Regulation ("**GDPR**") ((EU) 2016/679), and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time; (ii) all applicable marketing legislation including Directive 2002/58/EC ("**ePrivacy Directive**") as implemented by EU member states, Switzerland or in the United Kingdom (as may be applicable); (iii) any successor legislation to either GDPR or ePrivacy Directive or other applicable laws together with any legislation relating to data privacy in the relevant party's place of domicile or registration or in the territory in which Pegasystems provides services to the Client; (iv) all data protection, data privacy and marketing legislation, regulations, guidance, directions, determinations, codes of practice, circulars, orders, notices or demands issued by any supervisory authority and any applicable national, international, regional, municipal or other data privacy and data protection laws or regulations in the territory in which Pegasystems provides services to Client or which are otherwise applicable to provision of these services.

"Environment" means one of the Pega Cloud deployments provided by Pegasystems.

"European Data Protection Law" means, to the extent such law governs the processing of Client Personal Data under the applicable Schedule(s) to which Client or Pegasystems is subject, any Data Protection Law applicable in the EEA, the United Kingdom and Switzerland.

"Model Clauses" mean the standard contractual clauses approved by the European Commission for transfer of personal data being either:

1. Controller to processor clauses as approved by the European Commission in the Commission Decision 2021/915/EC dated June 4, 2021 (as amended and updated from time to time) ("**Model Clauses C2P**"), as set out in Attachment 3; or
2. Controller to controller clauses as approved by the European Commission in the Commission Implementing Decision (EU) 2021/915 dated June 4, 2021 (as amended and updated from time to time) ("**Model Clauses C2C**") as set out in Attachment 4; or
3. Any subsequent standard contractual clauses that may be adopted by authorized bodies.

"Instructions" means this Addendum and any further written agreement or documentation by way of which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data for that Data Controller.

"Pega Cloud" means Pegasystems' subscription-based offering of Pegasystems' software capabilities for Client to build and run their Client Application(s) on Pegasystems' operated environments.

"Professional Services" means professional services provided by Pegasystems pursuant to a Statement of Work for consulting, installation support, and access to training courses.

"Subprocessor" means any other Processor appointed by Pegasystems to Process Client Personal Data as set forth in Section 2 hereunder.

"Subscription Services" means the Pegasystems Software which is made available to Client for use on the Pega Cloud within the scope of use, including any enhancements, updates, upgrades, modifications, releases, Environments, data storage, or other services pursuant to an applicable Schedule.



The terms **"Data Controller"**, **"Data Subject"**, **"Personal Data"**, **"Process"**, **"Processing"**, **"Processor"**, and **"Personal Data Breach"** shall have the respective meanings given those words in the Regulation (EU) 2016/679 or any subsequent amendment thereto.

1. Data Processing. Each party agrees to comply with its obligations under Data Protection Law. Client agrees that its instructions to Pegasystems and its use of the services or Subscription Services under the applicable Schedule will comply with applicable Data Protection Law and will not cause Pegasystems to infringe applicable Data Protection Law. Client will ensure that it has the necessary consents, notices, and other requirements to enable lawful processing.

To the extent Data Protection Law applies to Pegasystems's processing of Client Personal Data, then the following terms apply:

- a. The parties intend that, except as provided in 1(b) below, in relation to such processing, Client is the controller and Pegasystems is a processor. The parties intend that, except as provided in 1(b) below, for purposes of CCPA, Pegasystems is the Service Provider (as defined in CCPA) and the Client is the Business (as defined in CCPA).
- b. The parties acknowledge that when the parties remain separate and independent controllers of Personal Data each party will comply with the obligations that apply to it as a controller and shall be individually and separately responsible for its compliance.
- c. The subject matter and details of the processing, including the type of Client Personal Data and categories of data subjects, are set forth in Annex I and in the applicable Schedule.
- d. Each party will comply with the obligations applicable to it pursuant to the Data Protection Law.
- e. The duration of the processing shall be from the date of this Addendum, (or, if later, from the date Client Personal Data is first processed through the provision of the use of the Pegasystems Subscription Services), until the Schedule expires or terminates.
- f. The purpose of the processing is to provide the Client with the services or Subscription Services pursuant to Data Protection Law as set forth in the applicable Schedule and any purpose compatible therewith.
- g. When acting as the controller, Client is responsible for the processing, access and use of Client Personal Data, and for responding to data subjects' requests concerning their rights under the Data Protection Law. If Client is unable to respond to or fulfill such requests, Pegasystems shall assist Client by providing appropriate technical and organizational measures, insofar as this is possible, for assisting Client with the fulfilment of the Client's obligation to respond to such requests.
- h. Client authorizes Pegasystems to process Client Personal Data to provide the Subscription Services in accordance with documented instructions of the Client and for the Permitted Purposes defined herein. Client agrees that Pegasystems may process Client Personal Data for (i) providing Subscription Services detailed in the Schedule and this Addendum; (ii) disclosures to Sub-processors; and (iii) as authorized by Data Protection Law or other applicable law (the **"Permitted Purposes"**). Pegasystems is reliant on Client's representations of the extent to which Pegasystems is authorized to process Client Personal Data.
- i. Client may provide additional instructions to Pegasystems about the processing of Client Personal Data. The parties shall negotiate in good faith with respect to any change in the services or Subscription Services and any additional fees that Pegasystems may charge to carry out such instructions. Each party consents to the other party using its Business Contact Data for contract management, payment processing, service offering, and business development purposes related to the Schedule and, when acting as a Controller, for such other purposes as set out in the using

party's privacy policy. For such purposes, and notwithstanding anything else set forth in the Schedule or this Addendum, each party shall be a Data Controller with respect to such Business Contact Data and shall process such information in accordance with applicable Data Protection Law (including provision of notices and obtaining consents where applicable). For the avoidance of doubt, such Business Contact Data does not constitute Client Personal Data for purposes of this Addendum.

- j. Retention, return and/or deletion of any Client Data, including Client Personal Data, will be governed by the terms of the Schedule unless Data Protection Law requires Pegasystems to retain a copy of such Client Data.
- k. Pegasystems shall provide commercially reasonable assistance to Client in ensuring compliance with the Client's obligations regarding (1) the security of Client Personal Data and (2) data protection impact assessments and prior consultation; taking into account the nature of the processing carried out by Pegasystems and the information available to Pegasystems.
- l. The parties agree that the Model Clauses C2P set out in Exhibit A apply only if Client Personal Data, to which the European Data Protection Law applies, is transferred by Client located in the EEA to Pegasystems located in a country that is outside of the EEA for which there is no European Commission adequacy finding. For the purposes of Exhibit A, when Client is a Controller or a Subprocessor on behalf of a Controller, Pegasystems is the "**data importer**" and Client is the "**data exporter**". It is understood that where Client is acting as a Subprocessor on behalf of a Client, it would be considered as the data exporter (while being a data importer in its role as a Subprocessor) for Pegasystems and Pegasystems will act as a data importer. Where the SCCs are applicable, Pegasystems Inc. is the signatory to the SCCs. Where the Pegasystems entity that is a party to this Addendum is not Pegasystems Inc., (but is in such a country outside of the EEA for which there is no European Commission adequacy finding) that Pegasystems entity is carrying out the obligations of the data importer on behalf of Pegasystems Inc.
- m. For transfers of Personal Data originating in the United Kingdom, the SCCs shall be amended in accordance with the United Kingdom Addendum to the European Commission SCCs ("**United Kingdom Addendum**") published by the United Kingdom Information Commissioner's Office on its official website. For clarity, the United Kingdom Addendum shall apply concurrently with the SCCs.
- n. For transfers of Personal Data from Switzerland, the SCCs shall be modified in accordance with the statement of the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") of 27 August 2021. In particular, the FDPIC shall be the competent supervisory authority insofar as the data transfer is governed by the Swiss Federal Act on Data Protection ("**FADP**") (Clause 13); the law of the EEA country specified in the SCCs shall be the governing law (Clause 17); the courts of the EEA country as specified in the SCCs shall be the choice of forum (Clause 18), but this shall not exclude individuals in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c); and the SCCs shall protect the data of legal entities in Switzerland until the entry into force of the revised FADP. In the event of any conflict or inconsistency between the SCCs, if applicable, and this Addendum, the SCCs shall prevail.
- o. When both parties are independent controllers under GDPR, the Model Clauses C2C will apply. Where the Model Clauses C2C are applicable, Pegasystems Inc. is the signatory to the Model Clauses C2C and any other Pegasystems entity is carrying out the obligations on behalf of Pegasystems Inc.
- p. Annexes I (list of parties & description of transfer), II (Technical & Organizational Measures), III (list of Subprocessors) apply to all Schedules pursuant to which Pegasystems processes Client Personal Data.
- q. Where the European Data Protection Law applies the processing of Client Personal Data, and where

certifications and other information provided by Pegasystems are insufficient to respond to Client's request that Pegasystems demonstrate compliance with its obligations under GDPR Article 28, subject to Client and/or its representatives signing suitable undertakings of confidentiality, Pegasystems shall allow the Client and/or its representatives to conduct an audit once annually at a mutually agreed time of all procedures and documentation necessary to demonstrate Pegasystems' compliance with GDPR Article 28. Pegasystems shall cooperate with such audits in a reasonable manner.

- r. Incident Reporting. The incident reporting will apply as set forth in the applicable Schedule.

2. Subprocessors and Affiliates

- a. Processor shall maintain and make available to Client a list of all Subprocessors it engages. Client grants to Pegasystems the general authorization to engage the services of its Affiliates and Subprocessors set forth in Annex III to provide the Pega Cloud. For Professional Services Schedules, Client also grants to Pegasystems the right to engage Subprocessors identified in the applicable Schedule in the course of providing Professional Services. Client consents to the use of Subprocessors, including as concerns data transfers. Pegasystems shall inform Client by updating the Website specified in Annex III (and Client can subscribe to update notifications on the Website), or for Professional Services by notifying Client in writing, of any intended changes concerning the addition or replacement of the Subprocessors. Client will have fourteen (14) days from the date of such notice to object to the change. In the event of no objection, Client is deemed to have accepted the Subprocessor. If Client objects in good faith to the appointment or replacement of a Subprocessor, Client shall cooperate with Pegasystems in good faith in determining a replacement Subprocessor. If the parties are unable to agree on a replacement Subprocessor within a reasonable time period, Pegasystems or Client may terminate the affected Schedule(s) with immediate effect on written notice to the other party.
- b. Where Pegasystems engages the services of an Affiliate or Subprocessor for carrying out any part of the services or Subscription Services, it shall impose on that Subprocessor substantially the same data protection obligations as set forth herein, including sufficient guarantees to implement the technical and organizational measures appropriate for their processing obligations. Pegasystems shall be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the services of each Subprocessor directly under the terms of this Addendum and applicable Schedule.
- c. Pegasystems shall ensure that its personnel, and those of its Affiliates and Subprocessors, authorized to provide Subscription Services have committed themselves to appropriate obligations of confidentiality.

3. Security Risk Assessment

- a. Data Controller agrees to perform its risk assessment ("**Security Risk Assessment**") prior to submitting any Client Personal Data to determine whether or not security controls described in the applicable Schedule for Subscription Services provide an adequate level of security, taking into account the nature, scope and context and purposes of processing, the risks associated with the data and the applicable Data Protection Laws.
- b. Data Processor agrees to provide reasonable assistance to Data Controller by providing Data Controller information to assist with Data Controller's risk assessment.
- c. As described in the applicable Schedule, Data Controller uses its own sole discretion to implement discretionary controls in its Client Application and use of the Subscription Services or Professional Services in order to ensure a level of security appropriate to the risk.

4. Technical and Organizational Measures

- a. Taking into account the Data Controller Security Risk Assessment set forth above, Pegasystems has implemented and shall maintain appropriate technical and organizational security measures for the processing of Client Personal Data in the context of providing the Pegasystems services in such a manner (i) to ensure a level of security appropriate to the risk to the Client Personal Data when it is processed by Pegasystems; and (ii) to enable Pegasystems to assist Client in the fulfillment of its obligations to respond to requests from data subjects exercising their rights under Data Protection Law.
- b. Pegasystems shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the contract. Pegasystems shall ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. Pegasystems will not assess the content of Client Personal Data in order to identify information subject to specific legal requirements. Client is solely responsible for complying with incident notification laws applicable to Client and fulfilling any third-party notification obligations related to regulators and/or data subjects.

5. Data Residency and Data Transfer. Pegasystems offers geographically segmented data residency services specific to its Pega Cloud offering. For Pega Cloud, unless otherwise specified in the applicable Schedule, if Client selects a regional zone in the applicable region in the applicable Subscription Schedule, then Client Data, including all Client Personal Data, will be stored at a data center(s) in the applicable region and will not be transferred or accessed from outside of the applicable region except at the Client's instruction or in connection with a support request submitted by Client. Pegasystems may provide network monitoring and system provisioning activities for the Environments from its network operation centers located inside and outside of the applicable region.

6. Disclosures. To the extent legally permitted, Pegasystems shall: (i) promptly notify Client of any subpoena, judicial, administrative, or arbitral order of a government entity that relates to the Client Personal Data which Pegasystems is processing on behalf of Client; and, at Client's request, provide assistance reasonably requested by Client to respond to the demand in a timely fashion.

7. CCPA. If Pegasystems is processing Personal Data within the scope of the CCPA, Pegasystems makes the following additional commitments to Client. Pegasystems will process Personal Data on behalf of Client and not retain, use, share or disclose that data for any purpose other than for the purposes set out in this Addendum and as permitted under the CCPA, including under any "sale" exemption. In no event will Pegasystems sell any such data. These CCPA terms do not limit or reduce any data protection commitments Pegasystems makes to Client in the Schedule or this Addendum, between Pegasystems and Client.

8. Data Protection Contact. Data Protection Contact for Pegasystems is privacy@pega.com.

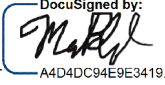
9. Notification of Personal Data Breach. Notification of Personal Data Breach shall be as set forth in the applicable Schedule.

[Signature Page Follows]




NOTWITHSTANDING THE SIGNATURES THIS ADDENDUM IS ONLY LEGALLY BINDING BETWEEN CLIENT AND THE PEGASYSTEMS CORPORATE ENTITY THAT SIGNED THE SCHEDULE(S) IN REFERENCE TO WHICH THIS ADDENDUM IS ENTERED INTO.

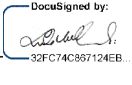
Pegasystems Inc.

Signature  DocuSigned by:
A4D4DC94E9E3419...
Name Mike Podol
Title Vice President
Date Signed 22 September 2021

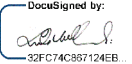
Pegasystems Limited

Signature  DocuSigned by:
AAA39F0B20ED42A...
Name Harvey Bishop
Title Managing Business Officer, EMEA
Date Signed 17 September 2021

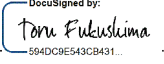
Pegasystems PTE Limited

Signature  DocuSigned by:
32FC74C887124EB...
Name Luke McCormack
Title VP & MD Pega Asia Pacific
Date Signed 16 September 2021

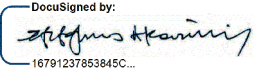
Pegasystems PTY Limited

Signature  DocuSigned by:
32FC74C887124EB...
Name Luke McCormack
Title VP & MD Pega Asia Pacific
Date Signed 16 September 2021

Pega Japan K.K.

Signature  DocuSigned by:
594DC9E543CB431...
Name Toru Fukushima
Title Managing Director
Date Signed 16 September 2021

Pegasystems Software (Beijing) Co. Limited

Signature  DocuSigned by:
16791237853845C...
Name Stathi Kouninis
Title VP, Finance
Date Signed 16 September 2021

Signed for and on behalf of the **Client**

Client Name _____
Signature _____
Name _____
Title _____
Date Signed _____

CONFIDENTIAL



List of Attachments:

1. Exhibit A: Standard Contractual Clauses (Controller to Processor)
2. Annex I: List of parties & description of transfer
3. Annex II: Technical and organizational measures
4. Annex III: List of Subprocessors

Exhibit A

Standard Contractual Clauses: Controller to Processor

SECTION I

Clause 1

Purpose and Scope

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- b. The parties
 - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')have agreed to these standard contractual clauses (hereinafter: '**Clauses**').
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and Invariability of the Clauses

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-Party Beneficiaries

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

- ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - v. Clause 13;
 - vi. Clause 15.1(c), (d) and (e);
 - vii. Clause 16(e);
 - viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the Transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking Clause

- a. An entity that is not a party to these Clauses may, with the agreement of the parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8**Data Protection Safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose Limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of Processing and Erasure or Return of Data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of Processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The parties shall consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management, and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, to notify the competent supervisory authority and the affected data subjects, considering the nature of processing and the information available to the data importer.

8.7 Sensitive Data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward Transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- a. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer.
- b. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question.
- c. the onward transfer is necessary for the establishment, exercise, or defence of legal claims in the context of specific administrative, regulatory, or judicial proceedings; or
- d. the onward transfer is necessary to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and Compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider relevant certifications held by the data importer.
- d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

The parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request

Clause 9

Use of Subprocessors

- a. GENERAL WRITTEN AUTHORISATION. The processor has the controller's general authorization for engagement of Subprocessors from the list published at: <https://www.pegacorp.com/subprocessors> (the "**Website**") to provide Pega Cloud. The data importer shall specifically inform (for Cloud by updated to the Website to which controller can subscribe) the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object.
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. x The parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data

importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- c. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the parties shall set out in Annex II the appropriate technical and organisational measures, considering the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the parties as regards compliance with these Clauses, that party shall use its best efforts to resolve the issue amicably in a timely fashion. The parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- a. Each party shall be liable to the other party/ies for any damages it causes the other party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one party is responsible for any damage caused to the data subject because of a breach of these Clauses, all responsible parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these parties.
- f. The parties agree that if one party is held liable under paragraph (e), it shall be entitled to claim back from the other party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- a. Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall be the competent supervisory authority in the EU Member State in which the data exporter is established.
Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data

is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, shall act as competent supervisory authority.

- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local Laws and Practices affecting Compliance with the Clauses

- a. The parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards
 - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two parties, the data exporter may exercise this right to termination only with respect to the relevant party, unless the parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the Data Importer in Case of Access by Public Authorities

15.1 Notification

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.)
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of Legality and Data Minimization

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider

that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-Compliance with the Clauses and Termination

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - ii. the data importer is in substantial or persistent breach of these Clauses; or
 - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
- d. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two parties, the data exporter may exercise this right to termination only with respect to the relevant party, unless the parties have agreed otherwise.
- e. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- f. Either party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without

prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing Law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The parties agree that this shall be the law of Germany.

Clause 18

Choice of Forum and Jurisdiction

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The parties agree that those shall be the courts of Member State in which the data exporter is established.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The parties agree to submit themselves to the jurisdiction of such courts.



ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Data Exporter: _____

Name (written out in full): _____

Contact person's name: _____

Contact persons' position: _____

Address: _____

Activities relevant to the data transferred under these clauses:

Other information necessary in order for the contract to be binding (if any):

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Data Importer: Pegasystems Inc.

Name (written out in full): Mike Podol

Position: Vice President

Address: One Main Street, Cambridge, MA 02142

B. DESCRIPTION OF TRANSFER

This Annex 1 forms part of the Addendum and Exhibit A (Standard Contractual Clauses). All definitions shall be as set forth in this Addendum. Any undefined term shall be as defined in applicable Data Protection Law.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Subjects

The Personal Data transferred concern the following categories of data subjects:

Individuals about whom Personal Data is provided or made available to Pegasystems or its affiliates or subprocessors via the Subscription Services by or at the direction of Client or its clients or end users.

Categories of Data

The Personal Data transferred concern the following categories of data:

Data relating to individuals provided to Pegasystems or its affiliates or subprocessors via the Subscription Services by or at the direction of Client or its clients or end users, or through the provision of Subscription Services.

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following special categories of data:

Data relating to individuals provided to Pegasystems or its affiliates or subprocessors via the Subscription Services by or at the direction of Client or its clients or end users, or through the provision of Subscription Services.

Processing Operations

The Personal Data transferred will be subject to the following basic processing activities:

Processing of Client or its clients' or end users' Personal Data as part of the provision of Subscription Services or Permitted Purposes by Pegasystems or its affiliates or subprocessors in accordance with the Addendum and the applicable Schedule.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex II forms part of the Addendum and Exhibit A (Standard Contractual Clauses). All definitions shall be as set forth in this Addendum. Any undefined term shall be as defined in applicable Data Protection Law. Description of the technical and organizational security measures implemented by the data importer.

Pegasystems will maintain technical, administrative, and physical security measures at least equivalent to those described in the applicable Schedule and, if applicable, the operating guides associated with the Pega Cloud as published from time to time on Pegasystems' web site at <https://community.pega.com/knowledgebase/pega-cloud>.

ANNEX III

LIST OF SUBPROCESSORS

This Annex III forms part of the Addendum and Exhibit A (Standard Contractual Clauses). All definitions shall be as set forth in this Addendum. Any undefined term shall be as defined in applicable Data Protection Law.

A list of Subprocessors is published at: <https://www.pega.com/subprocessors>. Clients can sign up for updates on this site.

For Professional Services, subprocessors will be listed in the applicable Statement of Work.