PROGRESS SOFTWARE CORPORATION DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into to ensure adequate safeguards with respect to the privacy and security of Personal Data passed from Customer to Progress for Processing on the Customer's behalf, as authorized by Customer in accordance with the requirements of the Data Protection Laws and Regulations.

This DPA is an addendum to each end user license agreement, master agreement, professional services agreement or other agreement between Customer and Progress pertaining to the licensing of products and/or the delivery of Services by Progress (each an "Agreement" and collectively the "Agreement(s)"). Each Agreement, as defined in the preceding sentence, includes all orders, schedules, exhibits, statements of work, addenda or other documents attached to, incorporated therein by reference or subsequently executed by the parties in accordance with the terms thereof.

By signing the DPA, Customer enters into the DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates.

During its performance of Services under the Agreement(s), Progress may Process Personal Data on behalf of Customer. This DPA specifies the parties' respective rights and obligations regarding the Processing by Progress of Personal Data supplied by Customer, and the parties agree to comply with the following provisions with respect to any such Personal Data, each acting reasonably and in good faith.

HOW TO EXECUTE THIS DPA

This DPA consists of two parts: the main body of the DPA and Appendix 1 (including Annexes 1 to 3).

The DPA and Standard Contractual Clauses in Appendix 1 have been pre-signed by Progress Software Corporation and each Progress Group member.

To complete this DPA, Customer must:

a) Complete the information in the "Customer" signature section and sign.
b) Complete the information regarding the data exporter in Annex 1 and sign.
c) Submit the completed and signed DPA to Progress via privacy@progress.com providing a return email address.

SCOPE AND APPLICATION OF THIS DPA

This DPA will apply to all Products and Services provided by Progress on behalf of Customer pursuant to the Agreement(s). For purposes of this DPA, Progress is the Processor (as defined below) and Customer is the Controller (as defined below). The scope of this DPA applies to:

- All Personal Data sent by or on behalf of the Controller to the Processor
- All Personal Data accessed by the Processor and its Affiliates, on the authority of the Controller

- All Personal Data otherwise received by the Processor, and its Affiliates, for Processing on the Controller's behalf

This DPA will be effective beginning on the day it is executed by Customer and will continue as long as any Agreement remains in effect. This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in Customer's Agreement (including any existing data processing addendum to the Agreement).

1. DPA DEFINITIONS

All capitalized terms not defined herein will have the meaning set forth in the applicable Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party hereto. "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.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations and (b) is permitted to use or benefit from the Services pursuant to the Agreement(s) between Customer and Progress, but has not signed its own order with Progress and is not the Customer.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer" means the customer entity that executes this document.

"Customer Data" means all electronic data processed by or on behalf of Customer, or an Authorized Affiliate, utilizing a product or Service provided by Progress under the Agreement.

"Data Protection Laws and Regulations" means all laws and regulations applicable to the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation or other use of Personal Data, including without limitation (i) the laws and regulations of the European Union, the European Economic Area and their member states (including without limitation the GDPR as well as any delegated acts and implementing acts), Switzerland and the United Kingdom; (ii) the California Consumer Privacy Act of 2018, sections 1798.100 through 1798.199 of the California Civil Code ("***CCPA***"), and (iii) the Brazilian Federal Law 13,709 ("***LGPD***").

"Data Subject" means an identified or identifiable natural person to whom the Personal Data relates.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the GDPR as incorporated into United Kingdom domestic law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 (the "***UK GDPR***").

"Personal Data" means any information relating to an identified or identifiable natural person or any other information definied as 'personal data' or 'personal information' under applicable Data Protection Laws and Regulations.

"Personal Data Breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed in connection with the provisioning of the Services.

"Processing" or "Process" means any operation or set of operations which is performed by Progress as part of the Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. The nature and purpose of the Processing, as well as the types of Personal Data and categories of Data Subjects covered by these Terms are set out under Appendix 1 to the Standard Contractual Clauses attached hereto as Appendix 1.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Progress" means the Progress Group member that is a party to the applicable Agreement with Customer.

"Progress Group" means Progress Software Corporation and its Affiliates.

"Services" means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the applicable Agreement where Progress Processes Customer's Personal Data.

"Standard Contractual Clauses" means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914&qid=1623940939861 ("***EU SCCs***"); and (ii) where the UK GDPR applies, the standard data protection clauses for processors adopted pursuant to or permitted under Article 46 of the UK GDPR ("***UK SCCs***"); in each case as may be amended, superseded or replaced from time to time. ;

"Third-Party Sub-processor" means a third-party subcontractor, other than Progress' Affiliate, engaged by Progress that Processes Customer's Personal Data.

Other terms have the definitions provided for them in the Agreement or as otherwise specified below.

2. Customer Processing Instructions

The Personal Data shall be confidential and shall be treated by Progress consistent with the confidentiality obligations contained in the Agreement. Accordingly, Progress shall only Process Personal Data on behalf of and in accordance with this DPA and the Agreement. Inter alia for the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed a documented instruction by Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable order(s); (b) Processing initiated by end-users in their use of the Service and (c) Processing to comply with other documented instructions provided by Customer where such instructions are consistent with the terms of the applicable Agreement.

Customer's instructions for the Processing of Personal Data will comply with Data Protection Laws and Regulations. Customer will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. If applicable law requires Progress (or, for the avoidance of doubt, any Sub-Processor) to conduct Processing inconsistent with any of

Controller's instructions, or if Progress believes that any instruction from Controller is in violation of, or would result in a violation of applicable law, Progress will notify Controller hereof without undue delay and prior to commencing the Processing.

The parties acknowledge and agree that regarding the Processing of Personal Data, Customer and its Affiliates permitted to use or benefit from the Services pursuant to the Agreement(s) between Customer and Progress are the Controllers, Progress is the Processor and that Progress may engage Sub-processors and Third-Party Sub-processors pursuant to the requirements set forth in the "Affiliates and Third-Party Sub-processors" section below.

3. Affiliates and Third-Party Sub-processors

Customer acknowledges and agrees that (a) members of the Progress Group and Progress' Affiliates may be retained as Sub-processors and (b) Progress, members of the Progress Group and Progress' Affiliates respectively may engage Third-Party Sub-processors regarding the provision of the Services provided that the applicable requirements set forth under the applicable Data Protection Laws and Regulations, Controller's instructions and this DPA (specifically this Section 3) – including, to the extent applicable, the Standard Contractual Clauses – are complied with at all times. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Progress has retained them to provide. Progress maintains a list of Progress' Affiliates and Third-Party Sub-processors that may Process Personal Data. Where Progress engages a Sub-processor for carrying out specific Processing activities on behalf of the Controller, the same data protection obligations and restrictions as set out in this DPA – including, insofar as applicable, the Standard Contractual Clauses – shall be imposed on that Sub-processor by way of a written agreement. Such agreement shall provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Laws and Regulations.

4. Notification of New Sub-processors and Objection Right for new Sub-processors

Progress will make available to Customer a current list of Sub-processors for the respective Services with the identities of those Sub-processors ("Sub-processor List") upon Customer request, such request to be not more than once per annum unless such information is required by reason of an enquiry by a data protection authority. Within ten (10) business days of Progress providing to Customer its list of Sub-processors, Controller may object to such change in writing if the new Sub-processor represents a substantial and unreasonable risk to the protection of Personal Data and may terminate the Agreement if, in Controller's reasonable discretion, Progress does not adequately address this objection.

Progress will be liable for the acts and omissions of its Sub-processors to the same extent Progress would be liable if performing the Services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. Rights of Data Subjects

Progress will, to the extent legally permitted, promptly notify Customer if Progress receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request").

Taking into account the nature of the Processing, Progress will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations.

In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Progress will upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Progress is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer will be responsible for any costs arising from Progress' provision of such assistance.

6. Personnel

Progress will ensure that its personnel and (as applicable) other persons authorized to process the personal data engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with Progress.

Progress will take commercially reasonable steps to ensure the reliability of any Progress personnel engaged in the Processing of Personal Data.

Progress will ensure that any access by a Progress Group member or Sub-Processor to Personal Data is limited to those personnel of the Progress Group member or Sub-Processor who require such access to perform the Agreement(s).

Members of the Progress Group have appointed a Data Protection Officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached by email via privacy@progress.com.

7. Security Measures

Progress will maintain appropriate technical and organizational security measures for the Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the Services ordered by Customer, may be specified in the Agreement.

Progress's present technical and organizational security measures are described in Appendix 2 to the Standard Contractual Clauses. Progress shall adapt these measures according to the development of regulations and technology.

Additionally, at the request of Controller, Progress will provide commercially reasonable assistance to Controller to ensure that any technical and organizational information security measures implemented by Controller satisfy the requirements of applicable Data Protection Laws and Regulations.

Where Controller determines it is obliged under applicable Data Protection Laws and Regulation to conduct privacy and/or security assessments, such as a data protection impact assessment ("DPIA") under the GDPR, Progress shall provide commercially reasonable cooperation and assistance with Controller's obligations. Additionally, if Controller determines that applicable Data Protection Laws and

Regulations requires Controller to consult with or seek guidance from a Supervisory Authority or other regulatory body prior to commencing any particular Processing, Progress shall provide commercially reasonable cooperation with and assistance to Controller in fulfilling its obligations. Any reasonable costs associated with Progress's rendering the assistance required by this paragraph shall be borne by Customer.

8. Audit Rights

The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon Customer's request, and subject to the confidentiality obligations set forth in the applicable Agreement, Progress will make available to Customer (or Customer's independent, third-party auditor that is not a competitor of Progress) information regarding the Progress Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications to the extent Progress makes them generally available to its customers.

Customer may contact Progress in accordance with the "Notices" section of the applicable Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer will reimburse Progress for any time expended for any such on-site audit at Progress' or the applicable Progress Group member's then-current professional services rates, which will be made available to Customer upon request.

Before the commencement of any such on-site audit, Customer and Progress will mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer will be responsible. Customer agrees that the scope of the audit shall be limited to matters specific to Customer. All reimbursement rates will be reasonable, considering the resources expended by Progress.

Customer will provide Progress with copies of any audit reports generated in connection with any audit under this Section, unless prohibited by Applicable Law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Customer will promptly notify Progress with information regarding any noncompliance discovered during the course of an audit and Progress will have the opportunity to remediate and rectify any issues identified within 30 days.

9. Incident Management and Breach Notification

Progress maintains security incident management policies and procedures and will notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Progress or its Sub-processors and Third-party Sub-processors, of which Progress becomes aware (a "Customer Data Incident"). Progress shall provide information necessary and requested by Controller to investigate the Security Incident. The Parties are aware that Data Protection Laws and Regulations may impose a duty to inform the Supervisory Authority or affected Data Subjects in the event of a Personal Data Breach. Processor shall assist Controller in providing notice to the Supervisory Authority and affected Data Subjects where such breach is likely to result in risk to the rights and freedom of a natural person. Progress will exercise reasonable efforts to identify the cause of such Customer Data Incident and

take those steps as Progress deems necessary and reasonable in order to remediate the cause of such Customer Data Incident to the extent the remediation is within Progress' reasonable control. The obligations herein will not apply to incidents that are caused by Customer or Customer's users.

For purposes of this section, the term "Customer Data Incident" as described in the preceding paragraph is further defined to mean the misappropriation or unauthorized Processing of Personal Data located on Progress' systems or cloud services environment, including misappropriation or unauthorized Processing of Personal Data by a Progress employee or a Third-party Sub-processor, that materially compromises the security, confidentiality or integrity of such Personal Data.

Customer agrees that: (i) an unsuccessful Customer Data Incident attempt will not be subject to this Section. An unsuccessful attempt is one that results in no unauthorized access to Customer's Personal Data or to any of Progress' equipment or facilities and any Third-party equipment or facilities storing Customer's Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and (ii) Progress' obligation to report or respond to a Customer Data Incident under this Section is not and will not be construed as an acknowledgement by Progress of any fault or liability with respect to the incident.

10. Retention and Disposition of Customer Data

Progress will return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data including existing copies and backups in accordance with the procedures and time periods specified in the applicable Agreement(s), unless the retention of the data is required for legal and regulatory purposes.

If the applicable Agreement does not provide guidance on retention and disposition of Customer Data, Progress will return and, to the extent allowed by applicable law, delete Customer Data within a commercially reasonable period of time, unless the retention of the data is required for legal and regulatory purposes.

The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses will be provided by Progress to Customer only upon Customer's request.

11. Legal Disclosure

Except as otherwise required by law, Progress will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority ("Demand") that it receives and which relates to the Processing of Personal Data. At Customer's request, Progress will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Progress has no responsibility to interact directly with the entity making the Demand except where Controller assesses, at its sole discretion, it is necessary to object to any request for access by a government by virtue of national law (such as the U.S. Cloud Act), and in such case Progress shall reasonably cooperate and assist Controller to compose such objection and to file such objection within the applicable timeframe. Such assistance and cooperation includes, but is not limited to, Progress binding itself to file such objection in its own name or on behalf of the Controller, where applicable, and to providing Controller with all required information to complete

the objection. Any reasonable costs associated with Progress's rendering the assistance required by this paragraph shall be borne by Customer.

12. Service Analyses

Progress may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (collectively "Service Analyses"). Progress may make Service Analyses publicly available. However, Service Analyses will not incorporate Customer Data or Personal Data in a form that could identify or serve to identify Customer or any Data Subject. Progress retains all intellectual property rights in Service Analyses.

13. Limitations of Liability

Each party's and all its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Progress, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the applicable Agreement unless specified below, and any reference in such section to the liability of a party means the aggregate liability of that party and all its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Progress' and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the applicable Agreement and each DPA will apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, will not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Neither Customer nor any of its Affiliates shall be entitled to recover more than once in respect of the same claim under this DPA.

Also, for the avoidance of doubt, each reference to the term "DPA" herein means this DPA including its Schedules and Appendices.

14. International Data Transfer; Standard Contractual Clauses

14.1 Progress shall comply with applicable Data Protection Laws and Regulations when transferring or onward transferring Personal Data across national borders.

14.2 Transfers from EEA Countries and the United Kingdom.

14.2.1 Any transfer of Personal Data from the European Economic Area ("EEA"), United Kingdom or Switzerland to a third country shall take place only if, in addition to complying with all other provisions of this DPA, the conditions set forth in this Section 14.2 are complied with. For the avoidance of doubt, the restrictions of this Section 14.2 also govern onward transfers of Personal Data within the third country, or from the third country to another third country.

14.2.2 The transfer of Personal Data is permitted to a third country for which the European Commission has decided that such third country, a territory or one or more specified sectors within that third country ensure(s) an adequate level of protection. To other countries, a transfer may only take place if appropriate safeguards are provided by other transfer mechanisms, such as Binding Corporate Rules; the Swiss-U.S. Privacy Shield; standard data protection clauses ("Standard Contractual Clauses") such as the European

Commission approved Standard Clauses for the Transfer of Personal Data to processors located outside the EEA ("C2P SCC"); or an approved certification mechanism or approved code of conduct within the meaning of Article 46(2)(e) and (f) of the GDPR. For the purposes of the UK SCCs: (ix) the Appendices or Annexes of the UK SCCs shall be populated with the relevant information set out in the Annexes to this Addendum; and (x) the UK SCCs shall be governed by the laws of and disputes shall be resolved before the courts of England and Wales

If and to the extent it is either agreed to by the parties or adjudicated that the specific basis used by the Parties for such data transfer will no longer be considered as providing appropriate safeguards for transfer of Personal Data from the EEA, United Kingdom or Switzerland to that third country, Parties agree to start negotiation about changing to another valid transfer mechanism. Controller may terminate the Agreement if Parties cannot agree to such a new transfer mechanism prior to the effective date of the final invalidation of the currently used transfer mechanism.

While Progress is certified to the EU-US Privacy Shield Framework and will maintain that certification and the commitments it entails, Progress does not rely on the EU-US Privacy Shield Framework as a legal basis for transfers of personal information in light of the judgment of the Court of Justice of the EU in Case C-311/18 and instead relies on the Standard Contractual Clauses as the legal basis for transfers of Personal Data from the EEA and United Kingdom to the US.

The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined above) of Customer established within the EEA, United Kingdom and/or Switzerland that have purchased Services on the basis of an order under the applicable Agreement. For the purpose of the Standard Contractual Clauses and this Section, the Customer and its Affiliates will be deemed to be "Data Exporters". The Parties agree that in the case of any inconsistencies between such Standard Clauses and this DPA, the Standard Clauses will prevail. For the avoidance of doubt, any provision of this DPA that merely goes beyond the clauses of the Standard Clauses without contradicting or altering them shall remain valid (to the extent permitted under applicable Data Protection Laws and Regulations and by competent Supervisory Authorities). Nothing in this DPA shall affect any Supervisory Authority's or Data Subject's rights under the Standard Clauses and applicable Data Protection Laws and Regulations.

15. Customer Data Subject to the CCPA

As used in this Section 15, "***Commercial Purpose***", "***Consumer***", "***Personal Information***", "***Sell***", and "***Service Provider***" have the meanings assigned to them in the CCPA.

If Customer Data comprises Personal Data subject to the CCPA ("***CCPA Covered Data***"), Progress is the Service Provider and, consistent with the requirements of the CCPA, shall not (a) Sell the CCPA Covered Data or (b) retain, use or disclose the CCPA Covered Data: (i) for any purpose, including any Commercial Purpose, other than for the specific purpose of providing and supporting the Product or Service or (ii) outside of the Parties' direct business relationship.

The Customer is responsible for responding to Consumer requests in relation to CCPA Covered Data (each, a "***Consumer Request***"). If Progress receives a Consumer Request then, to the extent legally permissible, Progress will advise the Consumer to submit the Consumer Request to the Customer. To the extent the Customer is unable through its use of the Product or Service to address a particular Consumer Request, Progress will, upon request and taking into account the nature of the CCPA Covered Data, provide reasonable assistance in addressing the Consumer Request (provided that Progress is

legally permitted to do so). Customer is responsible for verifying Consumer Requests in accordance with the CCPA.

16. Customer Data Subject to LGDP

If Customer Data comprises Personal Data subject to the LGPD ("***LGPD Covered Data***"), then Customer Personal Data, as the term is used in Sections 2 through 14 of this DPA above, shall be deemed to include LGPD Covered Data.

17. Parties to the DPA

Each Progress entity that is a party to the applicable Agreement is a party to this DPA. In addition, Progress Software Corporation is a party to the Standard Contractual Clauses in Attachment 1. If Progress Software Corporation is not a party to the Agreement, the "Limitations of Liability" section of this DPA will apply as between Customer and Progress Software Corporation, and in such respect any reference to 'Progress' will include both Progress Software Corporation and the Progress entity who is a party to the applicable Agreement.

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Progress entity that is party to the Agreement is party to this DPA. If the Customer entity signing this DPA has executed an Agreement with Progress or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Agreement and applicable amendments and renewals of that Agreement, and the Progress entity that is party to such Agreements is party to this DPA.

18. Legal Effect

This DPA will only become legally binding between Customer and Progress when fully executed by the parties. If this document has been electronically signed by either party such signature will have the same legal effect as a hand-written signature.

19. Order of Precedence

This DPA is incorporated into and forms part of the Agreement(s). For matters not addressed under this DPA, the terms of the Agreement(s) apply. With respect to the rights and obligation of the parties, in the event of a conflict between the terms of the Agreement(s) and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

Customer:

Signature:

By:

Title:

Date:

Progress Software Corporation

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Chief Legal Officer

Date: October 11, 2021

Progress Software do Brasil Ltda.

Signature: DocuSigned by: Bruno Manhaes 7A5EEE0F54C3450...

By: Bruno da Silva Manhaes

Title: Director

Date: October 11, 2021

Progress Software Corporation of Canada Ltd.

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software GmbH (Austria)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software N.V. (Belgium)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software E.A.D. (Bulgaria)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Executive Director

Date: October 11, 2021

Progress Software A/S (Denmark)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Oy (Finland)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software S.A.S. (France)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Gmbh (Germany)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Srl (Italy)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software B.V. (Netherlands)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Europe B.V. (Netherlands)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software AS (Norway)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software sp. z.o.o. (Poland)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software SLU (Spain)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Svenska AB (Sweden)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software AG (Switzerland)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Limited (UK)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Director

Date: October 11, 2021

Progress Software Pty. Ltd. (Australia)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Corporation Limited (Hong Kong)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Director

Date: October 11, 2021

Progress Software Development Private Ltd. (India)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Director

Date: October 11, 2021

Progress Software Corporation (S) Pte Ltd. (Singapore)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

Progress Software Technologies Ltd. (Ireland)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Director

Date: October 11, 2021

Progress Software Japan KK (Japan)

Signature: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483...

By: Stephen Faberman

Title: Director

Date: October 11, 2021

Chef Software UK Limited (UK)

Signature: DocuSigned by: Domenic Lococo B9361EBDB1E64B7...

By: Domenic LoCoco

Title: Director

Date: October 11, 2021

APPENDIX 1

STANDARD CONTRACTUAL CLAUSES – MODULE 2

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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 –Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – MClause 18(a) and (b)

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 in particular 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, in particular to notify the competent supervisory authority and the affected data subjects, taking into account 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:

(i) 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;

(ii) 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;

(iii) 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

(iv) the onward transfer is necessary in order 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 take into account 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.

(e) 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 sub-processors

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter 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 data exporter with the information necessary to enable the data exporter 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 data exporter), 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. 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 request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. 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, taking into account 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 as a result 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, as indicated in Annex I.C, 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) 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, as indicated in Annex I.C, 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, as indicated in Annex I.C, 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[1];

(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 minimisation**

(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.

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.

(d) 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.

(e) 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 the Netherlands.

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 the Netherlands.

(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*]

1. Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: The data exporter may, at its sole discretion transfer Personal Data to the data importer through its use of the software products and services licensed for its use by the data importer.

Signature and date: _____

Role (controller/processor): Controller

2. _____

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

1. Name: Progress Software Corporation

Address: 14 Oak Park Drive, Bedford, Massachusetts 01730, USA

Contact person's name, position and contact details: Stephen Faberman, Chief Legal Officer. Email: privacy@progress.com, Phone: (+1) 781 280 4000, Address as above.

Activities relevant to the data transferred under these Clauses: Progress Software Corporation, is a software company and cloud service provider which Processes Personal Data, where such data is Customer Data, upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Signature and date: DocuSigned by: Stephen H Faberman 4C6EB8B510F8483... October 11, 2021

Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customers, business partners, and vendors of the data exporter (who are natural persons)
- Employees or contact persons of data exporter customers, business partners, and vendors
- Employees, agents, advisors, contractors, or any user authorized by the data exporter to use the Service (who are natural persons)

Categories of personal data transferred

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- First and last name
- Business contact information (company, email, phone, physical business address)
- Personal contact information (email, cell phone)
- Title
- Position
- Employer
- ID data
- Professional life data
- Personal life data (in the form of security questions and answers)
- Connection data
- Localization data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data exporter may submit sensitive data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Information about security measures and safeguards is available at https://www.progress.com/security Data importer will not ask for, and data exporter will not transfer or otherwise provide, sensitive data to data importer.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis during the term of the Agreement, at the discretion of the data exporter.

Nature of the processing and Purpose(s) of the data transfer and further processing

Data importer will Process Personal Data as necessary to perform the Services pursuant to the Agreement and as further instructed by Data exporter in its use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of the Agreement, subject to any post-termination provisions relating to the return or destruction of Customer Data set out in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Detailed list of sub-processors, available on request.

C. **COMPETENT SUPERVISORY AUTHORITY**

As identified under Clause 13 or, if no Supervisory Authority is identified under that Clause, the Netherlands.

ANNEX II

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

Progress shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as detailed at https://www.progress.com/security.

Progress regularly monitors compliance with these safeguards. Progress will not materially decrease the overall security of the Service during a term of an Agreement.

ANNEX III

LIST OF SUB-PROCESSORS

A list of sub-processors for the Products/Services made available by Progress to Customer is available on request.