PTC Cybersecurity and Data Privacy Addendum (DPA).

This DPA forms part of the Agreement between Customer and PTC (as defined in the Agreement). Customer enters into this DPA on behalf of itself and to the extent required by Applicable Law, in the name and on behalf of its affiliates. For the purposes of this DPA only, unless indicated otherwise, the term "Customer" shall include Customer and its affiliates. All capitalizer terms not defined in this DPA shall have the mean as per the Agreement.

1. Purpose and scope

The parties agree that this DPA shall apply to all Processing of Customer Data including Personal Information undertaken by PTC on behalf of Customer and shall be supplemental to the terms of the Agreement. In the event of a conflict between the terms of the Agreement and this DPA, the terms of the DPA shall prevail.

2. Interpretation

2.1. Agreement shall mean any agreement between PTC and Customer under the terms of which PTC provides Services to Customer, including but not limited to PTC Cloud/SaaS Service Terms and Conditions; PTC Customer Agreement (License Agreement); Global Services Agreement.

2.2. Applicable Law shall mean GDPR, CCPA, LGDP and any other law or regulation concerning the processing of Personal Information and/or the protection of an individual's right to privacy or processing personal information.

2.3. CCPA shall mean California Consumer Privacy Act (as amended by the California Privacy Rights Act of 2020) [Ca. Civ. Code 1798.100, et seq.]

2.4. Controller shall mean the entity that determines the purpose and means of Processing of Personal Information.

2.5. Customer Data shall mean electronic data and information submitted by or for Customer to the Services, excluding non-PTC Applications and including Personal Information.

2.6. Customer Account Data shall mean personal data that relates to Customer's relationship with PTC, including the names or contact information of individuals (such as email address, phone number, title,) authorized by PTC to access Customer's account and billing information (including billing address) that Customer has associated with its account. Customer Account Data also includes any data PTC may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.

2.7. Customer Usage Data shall mean Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation user activity in relation to the types of Services Customer and its users use, the configuration of users' computers, and performance metrics related to their use of the Services, data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

2.8. Data Breach shall mean an incident that has resulted in a compromise of the security, confidentiality, availability or integrity of Customer Data or the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

2.9. GDPR shall mean General Data Protection Regulation (EU) 2016/679 of the European Parliament and country specific implementations of the regulation, including UK Data Protection Act 2018.

2.10. Individual shall mean an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to Personal Information.

2.11. LGPD shall mean Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) of Brazil.

2.12. Personal Information shall mean any information Processed by PTC on behalf of Customer relating to or linked or is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular Individual.

2.13. Processing shall mean any operation or set of operations which is performed on Customer Data, whether or not by automated means, such as, accessing, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

making available, alignment or combination, restriction, erasure or destruction.

2.14. **Standard Contractual Clauses** shall mean European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and applicable approved amendments to cover the transfer of personal data from Switzerland.

2.15. **UK International Data Transfer Agreement** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in Applicable Law or in a way that prejudices the fundamental rights or freedoms of individuals.

3. Purpose Limitation

PTC shall process Customer Data only for the specific purpose(s) of providing the Services, unless it receives further instructions from Customer. PTC shall not: (i) sell Customer Data; (ii) retain, use, or disclose Customer Data for a commercial purpose other than providing the Services or as described in this DPA; nor (iii) retain, use, or disclose the Customer Data outside of the Agreement. PTC shall not (and shall not permit any third party to) possess or assert any lien, encumbrance or other interest against or to any Customer Data.

4. Duration of the Processing

Processing of Customer Data by PTC shall only take place for the duration of the Agreement (including this DPA).

5. Security of Processing

5.1 PTC has established and during the term of the Agreement will maintain the technical and organizational measures specified in Annex II to ensure the security of Customer Data and protect Customer Data against a Data Breach. In assessing the appropriate level of cybersecurity, the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved have been taken into account.

5.2 PTC shall only grant access to Customer Data to members of its personnel and sub-processors to the extent strictly necessary for the provision of the Services. PTC shall ensure that persons authorized to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. PTC will regularly train personnel having access to Customer Data in applicable cybersecurity and data privacy measures. PTC will ensure that such access to and processing of Customer Data is limited to the extent strictly necessary for the provision of the Services.

5.3 Without prejudice to any existing contractual arrangements between the Parties, PTC shall treat all Customer Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing Customer Data of its confidential nature.

6. Audit

6.1 PTC is regularly audited by independent third-party auditors and/or internal auditors to verify the adequacy of its cybersecurity and privacy technical and organizational measures. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with PTC, PTC shall i) supply a summary copy of its audit report(s) to Customer; and ii) provide written responses to all reasonable requests for information made by Customer related to its Processing of Customer Data, including responses to information security and audit questionnaires, that are necessary to confirm PTC's compliance with this DPA and Applicable Law, provided that Customer shall not exercise this right more than once per calendar year. Where PTC has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, PTC agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement.

6.2 Where required by Applicable Law and only to the extent that in Customer's reasonable opinion, compliance with this DPA and Applicable Law has not been demonstrated through the exercise of its rights under Section 6.1 above, Customer and its authorized representatives may conduct audits, including inspections, during the term of the Agreement to establish PTC's compliance with the terms of this DPA, any such audit (or inspection) must be conducted during PTC's regular business hours, on reasonable notice. PTC and Customer shall agree the scope of the audit including timing and duration, of the audit and the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of PTC.

6.3 This Section 6 shall be subject Customer and its independent inspectors, as applicable entering an NDA to protect the confidentiality of all information disclosed and made available in the course of demonstrating compliance with this DPA and Applicable Law.

7. Notification of Data Breach

7.1 PTC has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Customer Data. PTC will promptly define escalation paths to investigate such incidents in order to confirm if a Data Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Data Breach, mitigate any possible adverse effects and prevent a recurrence. In the event of a Data Breach and taking into account the nature of Processing and the information available, PTC shall cooperate with and assist Customer to comply with its obligations under Applicable Law.

7.2 In the event of a Data Breach, PTC shall notify Customer without undue delay and in any event within 72 hours of PTC becoming aware of the Data Breach. Such notification shall contain, at least:

(a) "What Happened," a description of the nature of the Data Breach, the date and time at which it was first identified, and its likely consequences to the extent known;

(b) "What Information Was Involved," where possible, the nature of the Customer Data affected, the categories and approximate number of Individuals and data records concerned where known;

(c) "What We Are Doing," the measures taken or proposed to be taken to address the Data Breach, including to mitigate its possible adverse effects;

(d) "What You Can Do" being measures that PTC recommends Customer take to mitigate the effect of the Data Breach;

(e) "For More Information" the details of a contact point where more information concerning the Data Breach can be obtained.

7.3 Where, and insofar as, it is not possible to provide all this information at the same time, further information shall be provided, as it becomes available, without undue delay.

7.4 Unless required by Applicable Law, PTC shall not notify any individual or any third party other than law enforcement, forensic investigators, insurance providers or legal counsel of Customer's name or identity in association with any Data Breach without first consulting with, and obtaining Customer's written consent, which shall not be unreasonably denied. To the extent the Data Breach impacts other customers of PTC, a general public statement may be made as long as Customer's identity is not disclosed.

8. Processing of Personal Information

8.1 The parties expressly agree that the processing of Personal Information is not per se the subject of the Services. However, the parties acknowledge that it cannot be fully excluded that PTC may be provided with Personal Information to a certain extent. The terms of this DPA shall thus regulate the processing of Personal Information carried out by the PTC on behalf of Customer, due to the disclosure of such Personal Information. With respect to the Personal Information, Customer is responsible for i) ascertaining the legal basis for Processing, ii) ensuring that individuals are provided with all applicable privacy notices and iii) obtaining any consents where required under Applicable Law. Customer shall take reasonable steps to ensure that Personal Information does not include sensitive information such as health data, governmental IDs, credit or payment card information, or special category data as defined under Applicable Law. The details of the Processing operations, in particular the categories of Personal Information and the purposes of Processing for which the Personal Information is processed on behalf of Customer, are specified in Annex I.

8.2 PTC shall Process Personal Information only on documented instructions from Customer. The Agreement (including this DPA) constitutes such initial documented instructions. PTC will use reasonable efforts to follow any other Customer instructions, as long as they are required by Applicable Law, technically feasible and do not require changes to the performance of the Services. If any of the before-mentioned exceptions apply, or PTC otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Applicable Law, PTC will immediately notify Customer (e-mail permitted).

8.3 PTC may also process Personal Information where required to do so by Applicable Law. In such a case, PTC shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

8.4 Customer shall have the sole responsibility for the accuracy, quality, and legality of Personal Information and how Customer acquired the Personal Information. It is therefore the responsibility of Customer to ensure that Personal Information is collected and transmitted to PTC in compliance with Applicable Laws, in particular, to have a legal basis for Processing and to properly inform the Individuals of the collection and processing of their Personal Information.

9. Use of sub-processors

9.1 PTC has Customer's general authorization for the engagement of sub-processors to process Personal Information where strictly necessary for the performance of the Services. Customer approves those sub-processors listed at https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions. PTC shall inform Customer, in writing of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving Customer sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). PTC shall provide Customer with the information necessary to enable Customer to exercise the right to object.

9.2 Where PTC engages a sub-processor, it shall do so by way of a contract which imposes on the sub-processor, in substance, the same Processing and cybersecurity obligations as PTC's obligations under this DPA.

9.3 PTC shall remain fully responsible to Customer for the performance of the sub-processor's obligations in accordance with this DPA. PTC shall notify Customer of any failure by the sub-processor to fulfil its contractual obligations.

10. International Transfers of Personal Information

10.1 As a global company PTC may need to Process Personal Information out of the country that the Customer or the Individuals are located. All such transfers of Personal Information shall be in accordance with Applicable Law, and PTC shall ensure appropriate safeguards are maintained, the rights of Individuals are enforceable and effective legal remedies are available.

10.2 **EEA and Swiss UK Personal Information:** The parties agree that the Standard Contractual Clauses will apply to Personal Information that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland or UK that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the applicable competent authority) as providing an adequate level of protection for personal data. For transfers of Personal Information from the EEA that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed in accordance with Annex III

10.3 Where PTC's Binding Corporate Rules: Processor Policy applies, all provisions of the Binding Corporate Rules: Processor Policy are incorporated in this DPA by reference and shall be binding and enforceable by Customer as if they were set forth in this DPA in their entirety. In the event of any conflict or inconsistency between this DPA and the Binding Corporate Rules: Processor Policy, Binding Corporate Rules: Processor Policy shall prevail.

Order of precedence. Where more than one transfer mechanism applies as between the Customer (and/or Customer Affiliates) and PTC, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) Binding Corporate Rules: Processor Policy, and (ii) the Standard Contractual Clauses.

10.4 **UK International Data Transfer Agreement.** The UK International Data Transfer Agreement will apply to Personal Information that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is: (a) not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data and (b) not covered by the PTC's Binding Corporate Rules. For transfers of Personal Information from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this DPA by this reference) and completed as per Annex III.

10.5 **Other International Transfers:** Where PTC may be processing Personal Information on behalf of a Customer established in in a non-EEA country, Switzerland or the UK, PTC shall ensure that the transfer occurs in accordance with Applicable Law. This includes transferring the Personal Information to a recipient that has achieved binding corporate rules in accordance with Applicable Law, or to a recipient who has executed standard contractual clauses as adopted or approved by the applicable data protection authority.

11. Assistance to Customer with regard to Data Privacy Obligations

11.1 PTC shall promptly notify Customer of any request it has received from an Individual to exercise their rights under Applicable Law. It shall not respond to the request itself, unless authorized to do so by Customer.

11.2 The taking into account the nature of the Processing and the information it has available, PTC shall assist a) Customer in fulfilling its obligations to respond to an Individual's requests to exercise their rights, and b) Customer's compliance with the following obligations. In fulfilling its obligations, PTC shall comply with Customer's reasonable instructions:

(a) the obligation to carry out a risk assessment concerning the Processing of Personal Information, and/or an assessment of the impact of the envisaged Processing operations on the protection of Personal Information (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of Individuals;

(b) the obligation to consult the competent supervisory authority/ies under Applicable Law prior to Processing of Personal Information where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by Customer to mitigate the risk;

(c) the obligation to ensure that Personal Information is accurate and up to date, by informing Customer without delay if PTC becomes aware that the Personal Information it is Processing is inaccurate or has become outdated;

(d) the obligation to assist Customer in ensuring compliance with the obligations with regard to the security of Processing of Personal Information.

12. PTC as Controller:

Customer acknowledges and agrees that with respect to Customer Account Data and Customer Usage data, PTC is an independent Controller, not a joint Controller with Customer. PTC will process Customer Account Data and Customer Usage Data as a Controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, and compliance purposes and to manage its relationship with Customer; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer and Customer Data; (iv) for identity verification purposes;(v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Information to which PTC is subject; and (vi) as otherwise permitted under Applicable Laws and in accordance with this DPA and the Agreement. PTC may also process Customer Usage Data as a Controller to provide, optimize, enhance, and maintain the Services, including trouble shooting issues and developing, informing the development of new products and features, to the extent permitted by Applicable Laws. Any processing by the PTC as a Controller shall be in accordance with the PTC's privacy policy available at https://www.ptc.com/en/documents/policies/privacy.

13. CCPA Provision

As between Customer and PTC, for purposes of the CCPA, Customer is a "business" and PTC is a "service provider" and is receiving Personal Information for business purposes. PTC will not "sell" Personal Information to any "third party" and shall not retain, use or disclose any Personal Information except as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. For these purposes, "business", "service provider", "third party" and "sell" have the meaning ascribed to it in Section 1798.140 of the CCPA. PTC certifies that it understands the restrictions in this Section 13 and will comply with them.

14. Non-compliance with this DPA and termination

14.1 Without prejudice to any provisions of Applicable Law, if PTC is in breach of its obligations under this DPA, Customer may instruct PTC to suspend the Processing of Customer Data until PTC complies with this DPA or the

Agreement is terminated. PTC shall promptly inform Customer in case it is unable to comply with this DPA, for whatever reason.

14.2 Customer shall be entitled to terminate the Agreement insofar as it concerns Processing of Customer Data if:

(a) the Processing of Customer Data by PTC has been suspended by Customer pursuant to Section 14.1 and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension.

(b) PTC is in substantial or persistent breach of this DPA or its obligations under Applicable Law;

14.3 The liability of each party and each party's affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Any claims against PTC or its affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Individual or of any competent supervisory authority.

15. Retrieval and Deletion of Customer Data

Upon termination or expiration of the Agreement, Customer may export Customer Data as described in the Agreement, or where Customer Data (including Personal Information) cannot be exported, PTC shall return the Customer Data to Customer. PTC shall delete all Customer Data approximately 30 days following termination, in accordance with the terms of the Agreement, unless Applicable Law requires continued storage of the Customer Data. Until the Customer Data is deleted or returned, PTC shall continue to ensure compliance with this DPA.

16. Miscellaneous

16.1 The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.

16.2 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Laws.

16.3 This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically upon deletion by PTC of the Customer Data in accordance with Section 15 of this DPA.

[remainder of the page is intentionally blank]

ANNEX I

Categories of data subjects whose Personal Information is processed

Customer may submit Personal Information to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Information relating to the following categories of Individuals:

- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Employees or contact persons of Customer's customers, prospects, business partners and vendors
- Customer's Users authorized by Customer to use the Services

Categories of Personal Information processed

Customer may submit Personal Information to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Information:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data.

Sensitive data processed (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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- None

Nature of the Processing

- collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction as may be necessary for the provision of the Services

Purpose(s) for which the Personal Information is processed on behalf of Customer

- Provision of the Services more specifically defined in the Agreement

Duration of the Processing

- Subject to section 7 of this DPA, the term of which PTC provides the Services under the Agreement and any extension to or renewal of such term.

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of Customer Data

"Network" means a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data linked together using Local Area Network (LAN), Wide Area Network (WAN).

"Security Controls" means any specific hardware, software, or administrative mechanisms necessary to enforce NIST 800-53, in accordance with the terms of this Agreement as methods for addressing security risks to information technology systems and relevant physical locations or implementing related policies. Security Controls specify technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement Security Policy elements relevant to specific groups, individuals, or technologies.

"Security Policies" means statements of direction for securing company information pertaining to security and mandating compliance with applicable laws and regulations.

"Security Procedures" means step-by-step actions taken to achieve and maintain compliance with NIST 800-53 and/or ISO27001 certification.

"Systems" means computer software, firmware, computer hardware (whether general or special purpose), telecommunications capabilities (including all voice, data and video networks) and/or other similar or related items of automated, computerized, and/or software.

To comply with its security obligations under the terms the Agreement and DPA, PTC will at all times: (i) have security processes in line with industry best standards such as ISO27001 certification or shall have implemented the "moderate" impact controls of National Institute of Standards and Technology (NIST) 800-53 security requirements; (ii) the security requirements, obligations, specifications, and event reporting procedures set forth in this DPA;

PTC:

1. Security Program and Governance

will at all times maintain a Security Program which includes:

(a) A CISO or security designee, managing the below requirements
(b) Security Policies, Security Procedures, and Security Controls;
(c) A security incident management program;
(d) A security awareness and training program for all employees supporting this engagement;
(e) A security change management program to promote stability and reliability of PTC's security environment during the security change process; and
(f) Business continuity and disaster recovery plans, including regular testing.
(g) A security risk assessment process to identify, assess, respond and implement risk treatment
(h) If Provider develops and provides software as part of this engagement, Provider will maintain secure software development lifecycle aligned with industry standards such as OWASP OPEN SAMM
(i) If Provider is providing cloud services (IaaS, PaaS, SaaS) as part of this engagement, Provider will align practices with the CSA CCM and SOC2 standards

2. Security by Design and Testing

PTC will maintain:

(a) A security architecture that reasonably ensures alignment and implementation of effective NIST 800-53 Security Controls;
(b) A system of effective firewall(s) and intrusion detection technologies necessary to protect data;
(c) Appropriate Network security design elements that provide for segregation of data;
(d) Procedures to encrypt information in transmission and storage;
(e) Procedures to ensure regular testing of PTC's security systems and processes;
(f) Database and application layer design processes that ensure website applications are designed to protect

Customer data that is collected, processed, and transmitted through such systems.

3. Monitoring and Patch management

PTC has established and during the term of the Agreement will maintain:

(a) Mechanisms to keep security patches current;
(b) Monitoring systems and procedures to detect attempted and actual attacks on or intrusions into Customer data;
(c) Procedures to monitor, analyze, and respond to security alerts;
(d) Use and regularly update of commercial state-of-the-art antivirus and anti-malware software; and
(e) Procedures to regularly verify the integrity of installed software.

4. Remote Access Control by PTC Authorized Users

PTC will enforce:

(a) Appropriate mechanisms for user authentication and authorization in accordance with a "need to know" policy;
(b) Controls to enforce rigorous access restrictions for remote authorized users, both PTC's and sub-processors as applicable;
(c) Timely and accurate administration of authorized user account and authentication management;
(d) Mechanisms to encrypt or hash all passwords;
(e) Procedures to immediately revoke accesses of inactive account/terminated/transferred authorized users;
(f) Procedures maintaining segregation of duties;
(g) Procedures to ensure assignment of unique IDs to each authorized user with computer access; and
(h) Procedures to ensure PTC-supplied defaults for passwords and security parameters are changed and appropriately managed.
(i) Reasonable application of Multi-Factor Authentication (MFA) for Systems related to Customer Statement of Work

5. Facility Access Control

PTC has established and during the term of the Agreement will enforce:

(a) Physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and protected in appropriate data centers;
(b) Appropriate facility entry controls are maintained to limit physical access to Systems;
(c) Procedures to ensure access to facilities is monitored and restricted on a "need to know" basis;
(d) Measures to protect against destruction, loss, or damage of Customer data and Customer dependent Systems due to potential environmental hazards, such as fire and water damage or technological failures; and
(e) Controls to physically secure all Customer sensitive information and to properly destroy such information when it is no longer needed.

ANNEX III

Standard Contractual Clauses

The following Modules of the Standard Contractual Clauses shall apply and are hereby entered into and incorporated by reference as between PTC Inc. (as data importer) and Customer (including Customer acting as a Controller on behalf of its Affiliates and other controllers to which the transfer relates, as applicable) (as data exporter).

MODULE ONE – Transfer Controller to Controller for transfers where Customer is a Controller and PTC Processes Personal Information as an independent Controller as per the DPA
MODULE TWO – Transfer Controller to Processor, for transfers of Personal Information to PTC as a Processor and MODULE THREE - Transfer Processor to Processor (where Customer is a Processor and PTC is a sub-processor)

With regard to the Standard Contractual Clauses the following shall apply:

- Clause 9 – Use of sub-processors.
    - MODULE TWO & MODULE THREE
        - OPTION 2, General Written Authorization,
        - 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-PTCs at least 30 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-PTC(s).
- Clause 17 – Governing law
    - MODULE ONE, TWO & MODULE THREE
        - OPTION 1,
        - These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of The Republic of Ireland
- Clause 18, - Choice of forum and jurisdiction
    - MODULE ONE, TWO & MODULE THREE
    - (b) The Parties agree that those shall be the courts of the Republic of Ireland.

Annex I to Standard Contractual Clauses

A. LIST OF PARTIES
    - 1 – The Data Exporter is Customer, on its own behave and on behalf of Controllers located in the European Union, the UK and Switzerland
    - 2 – The Data Importer is the PTC Inc, 121 Seaport Boulevard, Boston, MA 02021
      and the respective contact details for Customer and PTC in the Agreement shall apply.

B. DESCRIPTION OF THE TRANSFER
   Categories of data subjects whose personal data is transferred

    - Module 1 – Controller to Controller:
        - Individuals who are authorized by Customer to use PTC products and/or access PTC services being Customer's employees, consultants, subcontractors, suppliers, business partners and customers.
    - Module 2 – Controller to Processor
    - Module 3 – Process to Processor
        - Customer's employees, consultants, subcontractors, suppliers, business partners and customers. Other individuals whose personal data may be uploaded by Customer to the Services

   Categories of data subject whose personal data is transferred:

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

- Module 1:
  Name, Company, username, userID, organisation, business contact details, interactions with PTC's products and services such as log-files and incident reports. IP addresses, cookie data, device identifiers and similar device-related information.
- Module 2 and Module 3: Name, Company, organization, business contact details, interactions with PTC's products and services such as log-files and incident reports, and personal data uploaded to PTC's services. No sensitive data will be transferred

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

Continuous

Nature of the processing

Data Importer shall Process Personal Data as required to provide the Services as more specifically described in the Agreement, and as authorized by the terms of the Agreement (including DPA) and shall include:
collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction as may be necessary for Data Importer to provide 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.

Personal data will be deleted from Service on termination of the Service in accordance with the terms of the Agreement.

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

See: https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions

C. COMPETENT SUPERVISORY AUTHORITY

- Identify the competent supervisory authority/ies in accordance with Clause 13
  - the competent supervisory authority shall be the Data Protection Commission of the Republic of Ireland.

Annex II to Standard Contractual Clauses - Technical and Organizational Measures.

Annex II to the DPA shall apply

UK - International Data Transfer Agreement

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in Paragraph A to this Annex III.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Paragraph B to this Annex III.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Paragraph A to this Annex III.
2. The description of the transfer is set forth in Paragraph A (Nature of Processing) Annex III.
3. Annex II (Technical and Organizational Security Measures) shall apply as Annex II to the UK International Data Transfer Agreement
4. The list of sub-processors is located at https://www.ptc.com/-/media/Files/PDFs/legal-agreements/fy18/PTC-Inc-List-of-Sub-processors.pdf.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.5 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms), the Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.