PTC Data Processing Terms & Conditions

In the provision of certain services under the terms of the Principle Agreement(s) as defined below, Customer, as controller will require PTC to process certain personal data received from Customer.

The parties agree that these terms and conditions shall apply to all such processing undertaken by PTC on behalf of Customer and shall be supplemental to the terms of the Principal Agreement.

1. Appointment

Customer as controller of certain personal data appoints PTC as processor to process the personal data listed in the Schedule(s) (the "Data") for the purposes also described in the Schedule(s) (or as otherwise agreed in writing by the parties) (the "**Permitted Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

2. Definitions

In these terms and conditions, the following terms shall have the following meanings:

(a) "**Principal Agreements**": Any agreement between PTC and Customer under the terms of which PTC provides services or licenses to Customer, including but not limited to PTC Cloud/SaaS Service Terms and Conditions; PTC Customer Agreement (License Agreement); Global Services Agreement; orders for PTCUniversity training including e-learning;

(b) "**controller**", "**processor**", "**data subject**", "**personal data**", "**personal data breach**" "**processing**" (and "**process**") and "**special categories of personal data**" and **"supervisory authority"** shall have the meanings given in Applicable Data Protection Law; and

(c) "**Applicable Data Protection Law**" shall mean, where personal data of EU residents is processed (i) prior to 25 May 2018, the EU Data Protection Directive (Directive 95/46/EC); (ii) on and after 25 May 2018, the EU General Data Protection Regulation (Regulation 2016/679), and (iii) where personal data of non-EU residents is processed any applicable privacy law in the relevant jurisdiction.

All other terms shall be as defined in the applicable Principle Agreement.

3. International transfers

As a global company PTC may need to transfer personal data out of the country that the Customer or the data subjects are located. All such transfers shall be in accordance with PTC's Global Data Transfer Agreement, or such other measures that permit the lawful transfer of personal data out of the EEA such as transferring the personal data to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.

4. Confidentiality of processing

PTC shall ensure that any person it authorises to process the personal data (an "Authorised Person") shall protect the personal data in accordance with have committed themselves to preserve the confidentiality of such personal data.

5. Security

PTC shall implement the technical and organisational measures as set out in the Schedule to protect the personal data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the personal data.

6. Subcontracting

Customer as controller consents to PTC engaging third party subprocessors to process the Data for the Permitted Purpose provided that: (i) PTC maintains an up-to-date list of its subprocessors at https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions, which it shall update with details of any change in subprocessors at least 10 days' prior to any such change taking effect; (ii) PTC imposes data protection terms on any subprocessor it appoints that require it to protect the personal data to the standard required by Applicable Data Protection Law; and (iii) PTC remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. Customer may object to PTC's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Customer may require PTC to suspend or terminate all processing activities (without prejudice to any fees incurred by or committed to by Customer under the terms of the Principal Agreement prior to suspension or termination).

7. Cooperation and data subjects' rights

PTC shall provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to PTC, PTC shall promptly inform Customer providing full details of the same.

8. Personal Data Breach

If it becomes aware of a confirmed personal data breach, PTC shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. PTC shall further take such any reasonably necessary measures and actions to remedy or mitigate the effects of the personal data breach and shall keep Customer informed of all material developments in connection with the personal data breach.

9. Deletion or return of Personal Data

Upon termination or expiry of the Principle Agreement, PTC shall (at Customer's election) destroy or return to Customer all personal data in its possession or control. This requirement shall not apply to the extent that PTC is

required by applicable law to retain some or all of the personal data, or to personal data it has archived on back-up systems, which personal data PTC shall securely isolate and protect from any further processing except to the extent required by such law.

10. Audit

Customer acknowledges that PTC is regularly audited for compliance with various internationally recognised standards as more specifically detailed in the Schedule(s) by independent third party auditors. Upon request, PTC shall supply a summary copy of its audit report(s) to Customer, which reports shall be subject to the confidentiality provisions these terms and conditions. PTC shall also respond to any written audit questions submitted to it by Customer, provided that Customer shall not exercise this right more than once per year. Notwithstanding the foregoing, in the event of an audit request directly from a Supervisory Authority, PTC shall always assist Customer in answering the request and organizing an audit.

11. Liability

Each party's liability to the other in respect of any individual claim for breach of contract, negligence, breach of statutory duty or otherwise in relation to these terms and conditions will be limited in accordance with the terms of the Principal Agreement.

12. General

The laws governing the Principle Agreement shall apply to these terms and conditions except in the case where personal data of EU citizens is being processed and the jurisdiction of the Principle Agreement is not that of a member state of the EU, in which case the laws of the Republic of Ireland shall apply in default.

These terms and conditions and the terms of the Principle Agreement referred to herein embody the whole agreement of the parties with respect to its subject matter.

Schedule:

Security Measures

Description of the technical and organisational security measures implemented by PTC as processor:

1. Secure user authentication protocols including:
    - Control user IDs and other identifiers
    - Provide a reasonably secure method of assigning and selecting passwords (or use an alternative authentication technology such as biometrucs or token devices)
    - Control data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect
    - Restrict access to active users and active user accounts only
    - Block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system
    - Restrict access to records and files containing personal information to those who need such information to perform their jub duties
    - Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with customer access, that are reasonably designed to maintain the integrity of the security of the access controls
2. Encrypt (to the extent technically feasible) all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly
3. Implement reasonable monitoring of systems, for unauthorized use of or access to personal information
4. Encrypt all personal information stored on laptops or other portable devices
5. Provide reasonably up-to-date firewall protection and operating system security patches for files containing personal information on a system that is connected to the Internet, designed to maintain the integrity of the personal information
6. Provide reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitons, or a version of such a software that can still be supported with up-to-date patches and virus defintions, and is set to receive the most current security updates on a regular basis
7. Educate and train employees on the proper use of the computer security system and the importance of personal information security

Ensure that any third party that may have access to the systems by way of providing services to PTC, but which are not providing data processing services, guarantee an equivalent level of security.

Data Security Certifications applicable to certain PTC Products or Services:

Cloud Services/SaaS – ISO27001(2013); SOC2 type 2

Technical Support: ISO9001.

DATA:

Data subjects

The Personal Data relating to the following categories of data subjects:

- 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.
- Other individuals whose personal data may be uploaded by Customer to PTC services or software.

Personal Data Categories
Name, Company, organisation, business contact details, interactions with PTC's products and services such as log-files and incident reports, training records and data that may be processed by PTC's products and other personal data that an individual may share with PTC.
IP addresses, cookie data, device identifiers and similar device-related information.

Permitted Purpose:
To DELIVER PTC SOFTWARE & SERVICES to Customer in accordance with the terms of the Principle Agreement and Customer's instructions.