ptc partner network

DATA PROCESSING TERMS AND CONDITIONS

These Data Processing Terms and Conditions are incorporated by reference into the PTC Partner Network Agreement.

1. Data Protection

1.1. Definitions: In these Data Processing Terms and Conditions, the following terms shall have the following meanings:

(a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in Applicable Data Protection Law; and

(b) "**Applicable Data Protection Law**" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC the Data Protection Directive; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament, the General Data Protection Regulation.

1.2. Relationship of the parties: The parties acknowledge that, pursuant to the Agreement, each party shall disclose to the other, personal data as described in Annex A to these Data Processing Terms and Conditions ("**Data**") for processing. Each party will process the copy of the Data in its possession or control as an independent controller (not as a joint controller with the other party).

1.3. Compliance with law. Each party shall comply with its obligations under Applicable Data Protection Law, and this Clause, when processing the Data. Neither party shall be responsible for the other party's compliance with Applicable Data Protection Law. In particular, each party shall be individually responsible for ensuring that its processing of the Data is lawful, fair and transparent, and shall make available to data subjects a privacy statement that fulfils the requirements of Applicable Data Protection Law. In particular, each party shall expressly state that the Data may be shared with PTC in the case of Partner and with members of PTC Partner Network in the case of PTC, solely for the Permitted Purpose (defined below).

1.4. Purpose limitation: Each party shall process the Data only for the purposes described in Annex A that are consistent with the consents or notices given by or to the data subjects or that are otherwise permitted under Applicable Data Protection Law. Partner shall only use any Data that is transferred to it by PTC support of the objectives of the Agreement and under no circumstances shall Partner use such Data for the promotion of products and services not supplied by PTC (the "**Permitted Purpose**").

1.5. International transfers: Partner shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Partner acknowledges that PTC put in place appropriate mechanisms to permit the lawful transfer of personal data out of the EEA either under the terms of a Global Transfer Agreement (based on the terms of Standard Model Clauses adopted by the European Commission) between all PTC entities or under the terms of Binding Corporate Rules approved by the European Data Processing Authorities.

1.6. Security: Both parties shall implement appropriate technical and organisational measures to protect the copy of the Data in their possession or control (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data. Such measures shall at a minimum, include the measures identified in Annex B to these Data Processing Terms and Conditions.

1.7. Third party processors: Each party may appoint one or more third party processors to process the Data for the Permitted Purpose on its behalf, provided: (i) it engages only processors that have implemented appropriate technical and organisational measures to protect the Data that as a minimum meet the measures set out in Annex B, and ensure the rights of the data subjects, in accordance with Applicable Data Protection Law; (ii) it engages such processors on contractual terms that set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of either party as the controller, and further provided that such contractual terms meet any mandatory requirements specified by Applicable Data Protection Law; and (iii) the recipient of the Data shall remain solely liable for any breach of this clause or of Applicable Data Protection Law that may be caused by its processors' processing of the Data.

1.8. Cooperation and data subjects' rights: Taking into account the nature of the processing, each party agrees to cooperate with the other as the controller in responding to individuals exercising their rights under the data privacy laws of the EEA and/or Switzerland.

Annex A

Data subjects

The Data to be processed concern the following categories of data subjects:
The Data relating to the following categories of data subjects:

- Employees of either party,
- Employees of customers and potential customers and, students attending training courses.

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 promote PTC SOFTWARE & SERVICES to potential customers, and to provide such software and services to customers and customer employees including without limitation technical support and training, license compliance
To manage the relationship between PTC and Partner including the training and performance management of Partner employees and the fulfilment of Partner programs.

The Data transferred may be disclosed only to the following recipients or categories of recipients:
PTC Group Companies and PTC's sub-processors.

Annex B
Description of Minimum Technical and Organisational Security Measures

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

8. 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.