PTC 数据处理条款与条件

根据下述“主协议”条款中对某些服务的规定，客户作为控制方会要求 PTC 处理接收自客户的某些个人信息。

双方同意这些条款与条件应适用于 PTC 代表客户进行的所有该类数据处理，并且应视为对主协议条款的补充。

1. 委托

客户作为某些个人信息的控制方委托 PTC 作为处理方出于附录同样所述之目的（或双方以其他方式书面协议之目的）（下称**“许可目的”**）处理附录中列出的个人信息（下称“信息”）。 各方须遵守适用的数据保护法中规定的适用义务。

2. 定义

在本条款与条件中，以下术语的定义解释如下：

(a) **“主协议”**：PTC 与客户根据 PTC 向客户提供服务或许可适用之条款而签署的任何协议，包括但不限于 PTC 云/软件即服务服务条款与条件；PTC 客户协议（许可协议）；全球服务协议；以及 PTCUniversity 培训（包括在线学习）规定；

(b) **“控制方”**、**“处理方”**、**“数据主体”**、**“个人信息”**、**“个人信息违反”**、**“处理”**（和**“处理”**）、**“个人信息特殊类别”**和**“监管机构”**的定义应与适用的数据保护法中的定义解释相同；

(c) **“适用的数据保护法”**：如果 (i) 2018 年 5 月 25 日之前处理欧盟居民的个人信息，则是指欧盟数据保护指令 (Directive 95/46/EC)；(ii) 如果 2018 年 5 月 25 日当天或之后处理欧盟居民的个人信息，则是指欧盟一般数据保护条例 (Regulation 2016/679)；(iii) 如果处理非欧盟居民的个人信息，则是指相关管辖区内所有适用的隐私法律。

其他所有术语应按适用的主协议中给出的定义解释。

3. 国际传输

作为一家全球性公司，PTC 可能需要将个人信息传输到客户或数据主体所在国家/地区以外的地区。所有该类数据传输均将根据 PTC 全球数据传输协议，或允许将个人信息合法传输到欧洲经济区以外的其他地区的其他该等法案进行，比如传输个人信息到已根据适用的数据保护法获得企业约束规则授权的接收者，或传输个人信息到已执行欧盟委员会采纳或批准的标准合同条款的接受者。

4. 数据处理的保密性

PTC 须确保 PTC 授权处理个人信息的任何人士（下称“经授权人士”）均已承诺且会按照该承诺尽力保护个人信息。

5. 安全性

PTC 应采取附录规定的技术和组织措施来保护个人信息，以免个人信息 (i) 遭受意外或非法损毁；(ii) 丢失、修改、未经授权的披露或访问。

6. 分包

客户作为控制方同意 PTC 委托第三方出于许可之目的处理数据，但前提是：(i) PTC 在 https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions 上发布 PTC 次级处理方的最新清单，而且如果次级处理方有任何变更，PTC 应在此类变更生效之前至少 10 天，使用次级处理方变更详细信息对清单进行更新；(ii) PTC 强制要求 PTC 委托的任何次级处理方实施数据保护条款，确保其按照适用的数据保护法要求的标准保护个人信息；(iii) 因 PTC 次级处理方的行为、错误或疏忽而违反本条款的任何情形，仍将由 PTC 承担责任。客户可在 PTC 委托或替换次级处理方之前反对该等委托或替换，但该反对必须基于与数据保护相关的合理理由。该种情况下，客户可要求 PTC 暂停或终止所有处理活动（不影响该暂停或终止前根据主协议的条款产生或客户承诺的任何费用）。

7. 协作与数据主体权利

PTC 应及时向客户提供合理协助（由客户承担费用），使客户能够对以下情形作出回应：(i) 数据主体提出请求，要求行使适用数据保护法赋予个人的任何权利时（包括在适用情况下对数据访问、纠正、反对、删除和可移植性的权利）；(ii) 收到数据主体、监管部门或其他第三方针对数据处理而发送或提出的任何其他信函、问询或投诉时。 如果该等请求、信函、问询或投诉是直接提交至 PTC，则 PTC 应立即通知客户并提供相关的完整详细信息。

8. 个人信息泄漏

如果 PTC 发现已确认的个人信息泄漏情形，PTC 应立即通知客户并提供合理信息，同时应与客户协作，使客户能够在适用的数据保护法要求的时限内，履行法律要求的数据泄漏上报义务。PTC 应进一步采取任何该等合理且必要的措施和行动来补救或缓解个人信息泄漏带来的影响，并应时时通知客户与该个人信息泄漏相关的所有重大进展。

9. 个人信息的删除或返还

主协议终止或到期后，PTC 应立即销毁或向客户返还（根据客户选择）PTC 持有或控制的所有个人信息。 该要求不适用于以下范围：PTC 依据适用法律需要保留部分或全部个人信息时；或者 PTC 已在其备份系统上存档的个人信息；但是，PTC 应严格隔离并保护该等个人信息，以免其被再次处理，但适用法律要求时除外。

10. 审计

客户承认 PTC 定期接受独立第三方审计师的审计，并且达到了附录中详细说明的各种国际公认标准。 如有要求，PTC 应向客户提供 PTC 审计报告的摘要副本，并且该报告应遵守条款与条件中的保密性规定。PTC 同时应对客户提交的任何书面审计问题作出答复，但客户每年只能行使一次该等权利。尽管有上述规定，如果监察机关直接提出审计要求，则 PTC 应始终协助客户答复该等要求并组织审计。

11. 责任

对于因违约、疏忽、违反法定义务而遭受的任何个体索赔，或是与本条款与条件相关的任何个体索赔，责任方对另一方所承担的责任仅限于主协议条款所载之责任。

12. 一般条款

主协议的管辖法律应同样适用于本条款与条件，但主协议的管辖权未覆盖所处理的欧盟公民个人信息所在的欧盟成员国时除外，在该种情形下，爱尔兰共和国的法律将为默认的适用法律。

本协议下所述之条款与条件和主协议的条款即构成双方就相关标的事项的全部协议。

附录：

安全措施

PTC 作为处理方所实施的技术和组织安全措施包括：

1. 用户身份验证安全协议，包括：
    - 控制用户 ID 和其他身份信息
    - 提供安全性得当的密码分配和选择方法（或使用其他身份验证技术，如生物测定或令牌设备）
    - 控制数据的安全密码，确保该密码的保存位置和/或格式不会影响被保护数据的安全性
    - 仅限活跃用户或活跃用户帐号拥有访问权限
    - 当有用户多次尝试访问特定系统并失败后，或是超出特定系统的许可尝试次数后，应禁用该用户
    - 仅限工作中要用到此类信息的人员可以访问含有个人信息的记录和文件
    - 向具有客户访问权限的每位人员分配专门设计用于维护访问控件安全完整性的唯一身份证明和密码（并非由供应商提供的默认密码）
2. 在技术可行的范围内，对要通过公共网络传输且包含个人信息的所有记录和文件进行加密，以及对要通过无线传输的所有数据进行加密
3. 对系统进行合理监控，防范未经授权使用或访问个人信息
4. 对存储在笔记本电脑或其他便携式设备上的所有个人信息进行加密
5. 为联网系统上包含个人信息的文件提供合理更新的防火墙保护和操作系统安全补丁且该等防火墙和补丁应专门设计用于维护个人信息完整性。
6. 提供合理更新版本的系统安全代理软件，该软件必需包含恶意软件防护、合理更新的补丁以及病毒定义；或提供仍能兼容更新补丁和病毒防护支持的该等软件版本，并且设置为定期接受最新的安全更新
7. 教育和培训员如何正确使用计算机安全系统以及使员工了解个人信息安全的重要性

确保虽未提供数据处理服务，但可能通过向 PTC 提供服务而具有系统访问权限的任何第三方，保证等同的安全级别。

适用于某些 PTC 产品或服务的数据安全认证：

云服务/SaaS - ISO27001(2013)；SOC2 (type 2)

技术支持：ISO9001。

数据：

数据主体

与以下数据主体类别相关的个人信息：

- 经客户授权可以使用 PTC 产品和/或访问 PTC 服务的个人，可为客户的员工、顾问、分承包商、供应商、业务合作伙伴和客户。
- 个人信息被客户上传至 PTC 服务或软件的其他个人。

个人信息类别
名称、公司、组织、业务联系人详细信息、与 PTC 产品和服务的交互（如日志文件和事故报告）、由 PTC 产品处理的培训记录和数据以及个人与 PTC 共享的其他个人信息。
IP 地址、cookie 数据、设备标识符和设备相关的类似信息。

许可目的：
根据主协议的条款和客户说明向客户交付 PTC 软件和服务。