PTC网络安全和数据隐私附录(DPA)

本附录构成客户与PTC所签订相关协议（定义见“相关协议”）的一部分。客户在适用法律规定的范围内，代表自身及其关联方并以关联方的名义订立本附录。在本附录中，除非另有说明，“客户”一词应包括客户及其关联方。本附录中未定义的所有大写字母术语应具有相关协议规定的含义。

1. 目的与范围

双方约定，本附录是相关协议条款的补充，适用于PTC代表客户对客户数据（包括个人信息）进行的所有处理活动。相关协议条款与本附录条款发生冲突时，应以本附录条款为准。

2. 定义

2.1. 相关协议：指PTC与客户之间签订的任何协议，包括但不限于《PTC云/SaaS服务协议》、《PTC客户协议（许可协议）》、《全球服务协议》等。PTC根据相关协议向客户提供服务。

2.2. 适用法律：指GDPR、UK GDPR、CCPA、LGDP、PIPL以及涉及个人信息处理和/或个人隐私权或个人信息处理权保护的任何其他法律法规。

2.3. **CCPA**：指《加州消费者隐私法案》（后经《2020年加州隐私权利法案》修订）/【《加州民法典》第1798.100条等】以及加利福尼亚州司法部长提供的任何相关法规或指南。

2.4. 控制方：指决定个人信息处理目的和处理方式的实体。

2.5. 客户数据：指由客户提供的与服务相关的电子数据和信息，但不包括非PTC应用程序信息，或由PTC代表客户处理的其他数据和信息，但不包括客户账号数据和客户使用数据。

2.6. 客户账户数据：指与客户和PTC合作关系有关的个人数据，包括经PTC授权可查看客户账户及相关 开票信息（包括开票地址）的任何自然人的姓名或联系信息（如电子邮件地址、电话号码、职务）。客户账户数据还包括PTC为了管理其与客户的关系、进行身份验证或相关法律法规另行规定的需要 收集的任何数据。

2.7. 客户使用数据：指公司收集并处理的与提供服务有关的服务使用数据，包括但不限于：与客户及其用户使用服务相关的活动，用户计算机的配置，与客户及其用户使用服务有关的性能指标，用于识别通信来源和目的地的数据、活动日志，以及用于优化和维护服务性能、调查和防止系统滥用的数据。

2.8. 数据泄露：指影响客户数据的安全性、保密性、可用性或完整性导致客户数据遭到非法破坏、丢失、更改、未授权披露或访问的事件。

2.9. **GDPR**：指欧洲议会的《通用数据保护条例》（法规编号：(EU) 2016/679）以及该条例在各个国家的实施情况。

2.10. 自然人：指已识别或可识别的自然人；可识别的自然人指可以直接或间接识别的自然人，具体参考与该自然人相关的标识符或其他相关定义。

2.11. **LGPD**：指巴西于2018年8月14日颁布的第13.709号法律《一般个人数据保护法》（后经2019年7月8日第13.853号法律修订）。

2.12. 个人信息：指客户数据中的直接或间接涉及或关联（或可合理认为直接或间接涉及或关联）某一特定自然人的任何信息。

2.13. 处理：指通过自动或非自动方式对客户数据进行的任何一个或一组操作，例如：访问、收集、记录、整理、结构化、存储、改编或更改、检索、咨询、使用，通过传输披露、传播或以其他方式提供、 调整或合并、限制、删除或销毁。

2.14. 服务：指协议中定义的任何服务。

2.15. 《标准合同条款》：指欧盟委员会于2021年6月4日发布的《关于根据欧洲议会和欧洲理事会第(EU)2016/679号条例及其经核准修订案（所述修订案旨在旨在规范瑞士的个人数据转移行为）向第三国传输个人数据的标准合同条款的实施决定》。

2.16. 英国附录：指由英国信息专员发布并于2022年3月21日生效的欧盟委员会《标准合同条款》的国际数据传输附录（B1.0版）。

2.17. 英国GDPR：指根据英国2018年《退出欧盟法案》第3章保留在英国法律中的GDPR。

2.18. PIPL：指中华人民共和国《个人信息保护法》（自2021年11月1日起施行）。

2.19. 本附录的解释不得违背适用法律规定的权利和义务，也不得损害任何自然人的基本权利或自由。

3. 目的限制

PTC应仅根据服务的要求以及本DPA的规定，处理客户数据。PTC不得：(i) 出售客户数据；(ii) 出于商 业目的保留、使用或披露客户数据（此处所述商业目的不包括提供服务，亦不包括本附录所述其他目的）；或(iii) 在违反相关协议的情况下保留、使用或披露客户数据。PTC不得（亦不得允许任何第三方）拥有或主张任何客户数据的任何留置权、抵押权或其他权益。

4. 处理期限

PTC只应在相关协议（及本附录）的有效期内处理客户数据。

5. 处理的安全性

5.1 PTC已经制定并（在相关协议有效期内）实施技术措施和组织措施（详见附件二），以确保客户数据的安全性并防止客户数据发生数据泄露事件。PTC在评估安全水平时，已经考虑到了技术水平、实施成本、处理的性质、范围、背景和目的，以及涉及的风险。

5.2 PTC应在提供服务的严格必要范围内，仅向其工作人员和分处理方授予客户数据的访问权。PTC应确保经授权处理客户数据的人员已经承诺保密，或同意承担相应法定保密义务。PTC将定期对有权限访问客户数据的人员提供相关网络安全和数据隐私保护方面的培训。

5.3 在不影响双方之间任何现有合同协议的情况下，PTC应将所有客户数据视为严格保密信息，并应将此保密性告知其所有参与处理客户数据的雇员、代理人和/或核准的分处理方。

6. 审计

6.1 PTC应定期接受独立的第三方审计员和/或内部审计员的审计，以确认其保护网络安全和隐私的技术措施和组织措施是否充分。PTC应按客户的要求：i)向客户提供审计报告的摘要副本；ii)书面答复客户提出的涉及客户数据处理的所有合理信息要求，包括回复用于确认PTC是否遵守本附录和适用法律所必需的信息安全与审计调查问卷，但客户每个日历年内提出此要求的次数不得超过一次。如果PTC已就文件所述的某项服务获得了ISO 27001认证以及根据SSAE 18编制的服务组织控制报告（“SOC2报告”），PTC同意在相关协议有效期内维持相关认证或标准，或其他适当且相当的替代认证或标准。

6.2 依据适用法律规定，仅当客户有理由认为行使上述第6.1款所述权利无法证明PTC遵守本附录和适用法律时，客户及其授权代表方可在相关协议的有效期内进行审计（包括检查），从而确定PTC是否遵守相关协议的条款。任何此类审计（或检查）必须在PTC的正常营业时间内进行，并应向 PTC提供合理通知。PTC和客户应商定审计范围、审计时间和审计期限，以及客户应负责的费用报销比例。考虑到PTC或其代表所花费的资源，所有报销比例均应合理。

6.3 依据本附录第6条，客户及其独立检查员应适时签订保密协议，以保护PTC在证明其遵守本附录和适用法律的过程中所披露和提供的所有信息的保密性。

7. 数据泄露通知

7.1 PTC已经实施控制措施和政策，以便发现和及时应对可能造成数据泄露的事件。PTC应及时确定此类事件的上报调查途径，确认是否已经真实发生数据泄露，采取用于确定数据泄露根源的合理措施，降低任何可能的不利影响，并防止再次发生同类事件。倘若发生数据泄露，PTC应考虑到处理性质和现有信息，与客户开展合作并协助其履行适用法律规定的义务。

7.2 一旦发生数据泄露，PTC应及时通知客户。无论任何情况，PTC通知客户的时间均应在其意识到数据泄露发生后的72小时内。在可能的情况下，该等通知应至少包括：

(a) “事件经过”：描述数据泄露的性质、首次发现数据泄露的日期和时间，以及已知的可能后果。

(b) “相关信息”：尽可能说明受影响的客户数据的性质，以及目前已知的自然人和相关数据记录的类别和大致数量。

(c) “当前行动”：PTC为解决数据泄露问题所采取或建议采取的措施，包括降低可能的不利影响。

(d) “行动建议”：PTC建议客户为降低数据泄露的影响而采取的行动。

(e) “更多信息来源”：指可以获得数据泄露更多相关信息的联络点详情。

7.3 倘若无法同时提供上述所有信息，PTC应在知悉进一步信息之后毫不迟延地通知客户。

7.4 除非适用法律有所要求，否则PTC在未事先咨询并获得客户的书面同意（客户不得无故拒绝同意）的情况下，不得因任何数据泄露事件将客户的名称或身份告知给除执法部门、法医人员、保险公 司或法律顾问以外的任何自然人或任何第三方。如果数据泄露事件影响到PTC的其他客户，那么 PTC在不披露客户身份的情况下可以作出一般性的公开声明。

8. 个人信息的处理

8.1 双方明确约定，个人信息的处理本身不是服务的主体。然而，双方确认，不能完全排除PTC在一定程度上收到客户个人信息的可能性。因此，鉴于客户可能向PTC披露个人信息，本附录的条款应适用于PTC代表客户处理个人信息的行为。对于个人信息，客户应：i) 确定处理的法律依据；ii) 确保向自然人提供所有适用的隐私通知；以及iii) 根据适用法律要求获得任何同意。客户应采取合理措施，确保个人信息不包括健康资料、政府核发之身份证、信用卡或支付卡信息等敏感信息或适用法律规定的特殊类别数据。附件一详细描述了个人信息的处理操作，特别是个人信息的类别，以及 PTC代表客户处理个人信息的目的。

8.2 PTC应仅根据客户的书面指示处理个人信息。 相关协议（包括本附录）构成了客户的初始书面指示。PTC应尽合理努力遵循客户的任何其他指示，但前提是客户的指示符合适用法律的有关规定，具有技术上的可行性，并且不要求改变服务的执行。倘若发生前述任何例外情况，或PTC因故无法遵循指示，或PTC认为某项指示违反了适用法律，PTC将立即通知客户（可以使用电子邮件发送通知）。

8.3 PTC还可依据适用法律的相关规定处理个人信息。在这种情况下，除非适用法律以保护重大公共利益为由禁止PTC对外发送通知，否则PTC应在处理个人信息之前将相关规定通知客户。

8.4 客户应对个人信息的准确性、质量、合法性以及客户获取个人信息方式承担全部责任。因此，客户应确保个人信息的收集和传输符合适用法律的相关规定。特别是，客户应有处理该等个人信息的法律依据，并通过妥善方式告知相关自然人其个人信息已收集并处理。

9. 分处理方的使用

9.1 PTC拥有客户的一般授权，在履行服务义务过程中，可在绝对必要的情况下，委托分处理方处理个人信息。客户批准的分处理方名单参见：https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions。PTC打算通过新增或更换分处理方的方式变更上述名单时，应至少提前30天通过书面形式通知客户，以便客户在聘用相关分处理方之前拥有足够的时间对名单的变更提出异议。PTC应向客户提供必要信息，确保客户能够行使异议权。

9.2 聘用分处理方时，PTC应与之签订合同。分处理方在该合同项下的个人信息处理和网络安全义务实际上应与PTC在本附录下的义务相同。

9.3 PTC应对分处理方代其履行本附录项下义务的表现，向客户承担全部责任。

10. 个人信息的国际传输

10.1 作为一家全球性公司，PTC可能需要在客户或自然人所在国以外地区处理个人信息。所有此类个人信息的传输均应符合适用法律，PTC应确保持续采取相关保障措施，确保自然人的权利可强制执行，也确保自然人可以获得有效的法律救济。

10.2 欧洲经济区和瑞士的个人信息。双方约定，如果客户将个人信息从欧洲经济区或瑞士传到PTC，无论直接或间接转移至欧洲经济区、瑞士以外任何国家或接收方。欧盟委员会（或相关主管机构（适用于瑞士输出的个人信息））认为该等国家或接收方无法对个人信息提供充分的保护，则适用《标准合同条款》。对于欧洲经济区输出的受限于欧盟《标准合同条款》的个人信息传输，欧盟《标准合同条款》应视为根据附件三订立（并通过引用纳入本附录）和缔结的协议。

10.3 若PTC的《约束性公司规则：处理方政策》适用，则《约束性公司规则：处理方政策》应视为通过引用方式纳入本附录，并且整体上如同本附录一样，对客户具有约束力和可执行性。若《约束性公司规则：处理方政策》与本附录之间存在任何冲突或不一致，则应以《约束性公司规则：处理方政策》为准。

优先顺序。若客户与PTC之间适用多种传输机制，则个人信息的传输将按照下列优先顺序适用单一传输机制：(i) 《约束性公司规则：处理方政策》；以及(ii)《标准合同条款》。

10.4 英国附录：双方约定，如果客户将个人信息从英国传到PTC，无论直接或间接转移至英国以外的 任何国家或接收方，而英国监管机构或政府机关认为该等国家或接收方无法对个人信息提供充分 的保护，则适用《英国附录》对于英国输出的受限于《英国附录》的个人信息传输，《英国附录》应视为根据附件三订立（并通过引用纳入本附录）和缔结的协议。

中国：双方同意，PTC 将把在中国境内（仅为本 DPA 之目的，不包括香港特别行政区、澳门特别行政区和台湾省）生成的客户数据存储于位于中国境内的服务器上。

10.5 在客户遵守以下条件的前提下，客户可以指示 PTC 在中国境外处理客户数据：

(a) 作为该等客户数据的控制方，客户应确保将客户数据传输至中国境外不违反适用法律，并应确保遵守所有适用的中国法律、法规及有关跨境数据传输的监管要求；

(b) 客户应根据适用法律要求，事先向相关数据主体提供通知，并取得有效的单独同意（如适用）；

(c) 在任何情况下，客户均应自行承担采取一切必要措施的全部责任，以遵守中国适用法律中有关数据跨境传输的法定要求；以及

(d) 遵守中国适用法律规定的其他数据跨境传输要求。

10.6 其他国际传输：如果PTC可能正在代表成立地位于非欧洲经济区国家、瑞士或英国的客户处理个人信息，那么PTC应确保相关传输符合适用法律。这包括将个人信息传输至已经根据适用法律建立《约束性公司规则》的接收方，或已经签署相关数据保护机构采用或批准的《标准合同条款》的接收方。

11. 在数据隐私义务方面对客户的协助

11.1 PTC应将自然人提交的关于行使其在适用法律项下相关权利的任何请求及时通知客户。除非得到客户的相关授权，否则PTC本身不得对此类请求作出回应。

11.2 鉴于处理的性质及掌握的信息，PTC应：a) 协助客户履行其义务，从而对自然人的行权请求作出回应；b)助力客户根据适用的法律，遵守下列义务。：

(a) PTC有义务对个人信息的处理进行风险评估，并且/或者在某类处理可能导致个人权利和自由面临高风险时，评估相关处理操作对个人信息保护的影响；

(b) 若数据保护影响评估结果表明，在客户未采取措施降低风险的情况下，处理过程将导致高风险，则PTC有义务在处理个人信息之前咨询主管监督机构；

(c) 若PTC知悉其正在处理的个人信息不准确或已经过时，则PTC有义务通过及时通知客户的方式来确保相关个人信息准确且最新；

(d) PTC有义务协助客户确保履行个人信息处理安全性相关的义务。

12. PTC作为控制方：

客户确认并同意：就客户账户数据和客户使用数据而言，PTC是独立控制方，而非与客户一起构成共同控制方。作为控制方，PTC将处理客户账户数据和客户使用数据，以期达到下列目的：(i) 管理与客户的关系；(ii) 执行公司的核心业务运作，如会计、合规目的、客户关系管理等；(iii) 监测、调查、预防和检测欺诈、安全事件和其他滥用服务的行为，并防止客户和客户数据遭受损害；(iv) 用于身份验证；(v)遵守

PTC处理和保留个人信息的相关适用法律或监管义务；以及(vi)符合适用法律、本附录和相关协议的有关规定。作为控制方，PTC还可在适用法律允许的范围内处理客户使用数据，从而提供、优化、增强和维护服务（如故障排除、开发创新等），为新产品和新功能的开发提供信息。PTC作为控制方进行的任何处理操作均应符合PTC的隐私政策，具体参见：https://www.ptc.com/en/documents/policies/privacy。

13. CCPA规定

依据CCPA规定，在客户和PTC之间，客户是一家“企业”，而PTC则是一家出于商业目的接收个人信息的“服务提供商”。除非为了依据相关协议向客户提供服务，或者为了依据相关协议和CCPA达成其他目的，否则PTC不得将个人信息“出售”或“分享”给任何“第三方”，亦不得保留、使用或披露任何个人信息。 上述条款中，“企业”、“服务提供商”、“第三方” 、“销售”和“分享”的定义参见CCPA第1798.140条。 PTC证明其了解本附录第13条所述的限制，并将遵守该等限制。

14. 违反本附录和协议终止

任何一方的关联方在本附录下的责任应受限于相关协议中关于责任排除和责任限制的规定。针对本附录项下PTC或其关联方的任何索赔，只能由作为协议一方的客户实体提出。无论任何情况，本附录或任何一方均不得限制或约束任何自然人或任何主管监督机构的权利。

15. 客户数据的检索和删除

相关协议终止或期满后，客户可立即按相关协议规定输出客户数据；或者，若客户数据无法输出时，PTC应将客户数据归还给客户。除非适用法律要求继续保存客户数据，否则PTC应在相关协议终止后大约30天内，按照相关协议的条款，删除所有的客户数据。在删除或归还客户数据之前，PTC应继续确保遵守本附录。

16. 其他

16.1 双方同意，本附录应取代双方此前可能已经签订的与服务有关的任何《网络安全和数据隐私附录》。

16.2 除非适用法律另有要求，否则本附录应受相关协议所述管辖法律和管辖权条款的管辖，并据其进行解释。

16.3 本附录和《标准合同条款》将在PTC根据本附录第15条删除客户数据的同时自动终止。

[以下无正文]

附件一

个人信息已处理的数据主体类别

客户可以向服务项目提交个人信息，其范围由客户自行决定和控制，其中可能包括但不限于与下列各类自然人有关的个人信息：

- 客户的雇员、代理人、顾问、自由职业者（皆为自然人）；
- 客户的客户、潜在客户、商业伙伴和供应商的雇员或联系人；
- 经客户授权可使用服务的用户；

已处理个人信息的类别

客户可以向服务项目提交个人信息，其范围由客户自行决定和控制，其中可能包括但不限于下列各类个人信息：

- 姓名；
- 职务；
- 职位；
- 工作单位；
- 联系信息（公司、电子邮件、电话、实际业务地址）；
- 身份信息；
- 位置；

已处理的敏感数据（如果适用）和适用的限制或保障措施，充分考虑到数据的性质和所涉及的风险，例如，严格的目的限制，访问限制（包括只有经过专门培训的员工才能访问），保存数据访问记录，限制转发或其他安全措施。

- *仅限 ServiceMax，指使用 ServiceMax Go 的工程师的实时地理位置数据。*
  适用的限制或保障措施：ServiceMax Go 在严格目的限制原则下处理位置数据：九项独立功能中的每一项仅为一项明确声明的目的读取位置数据，且其中八项功能仅获取交易性、一次性或限于会话期间的位置定位。持续后台采集仅存在于一项功能（位置历史记录）中，该功能默认关闭，且只能由客户自己的 ServiceMax 管理员启用；由调度员发起的位置请求亦受同一设置限制。技术措施包括：操作系统运行时权限模型作为外部控制机制；强制性的使用中提示（Android 前台服务通知、iOS 后台位置提示、应用内 toast 提示）；用户可控制的 1 至 24 小时暂停采集功能；采用 TLS 传输、OAuth 持有者令牌认证以及绑定租户的 X-Origin 标头；设备端凭据加密存储；成功上传后立即删除设备端缓存；以及由管理员设置缓存记录上限。位置历史记录仅传输至客户自己的 ServiceMax 同步网关——ServiceMax 不运营任何跨租户共享的位置数据存储——且不会向任何第三方分析或崩溃报告处理方传输技术人员坐标。地理围栏评估完全在设备端执行，不传输任何坐标。位置数据到达客户的 ServiceMax 实例后，其访问控制、访问日志和留存期限由 ServiceMax 平台的基于角色的权限模型管理，并由平台团队另行答复。~~无~~

处理的性质

- 为提供服务可能需要进行的收集、记录、组织、结构化、存储、改编或更改、检索、咨询、通过传输披露、传播或以其他方式提供、限制、删除或毁坏。

代表客户处理个人信息的目的

- 提供相关协议具体规定的服务

处理期限

- PTC　根据相关协议提供服务的期限，以及该期限的任何延长期或续期。



附件二

技术措施和组织措施（包括旨在确保客户数据安全性的技术措施和组织措施）

"网络"：指相互连接并可通过局域网（LAN）和广域网（WAN）共享数据的计算机、服务器、主机、网络设备、外围设备或其他设备的集合。

"安全控制措施"：指依据相关协议的规定，为强制执行NIST 800-53所需的任何具体的硬件、软件或管理机制，用于应对信息技术系统和相关物理位置的安全风险或实施相关政策。安全控制措施规定了技术、方法、实施程序和其他详细因素或其他流程，用于实施与特定群体、个人或技术有关的安全政策要素。

"安全政策"：指确保公司安全相关信息和确保适用法律法规合规性的方向性声明。

"安全程序"：指为实现并维持NIST 800-53和/或ISO27001认证而采取的分步行动。

"系统"：指计算机软件、固件、计算机硬件（无论是通用还是专用）、电信能力（包括所有语音、数据和视频网络）和/或其他类似或相关的自动化项目、计算机化项目和/或软件项目。

为了遵守相关协议和本附录规定的安全义务，PTC应始终：(i)拥有符合ISO27001认证等行业最佳标准的安全程序，或应实施美国国家标准技术研究所(NIST)800-53安全要求的"中等"影响控制措施；(ii)制定本附录中规定的安全要求、义务、规范和事件报告程序。

1. 安全计划和治理

PTC应始终维持包含下列内容的安全计划：

(a) 首席信息安全官或安全指定人员，负责管理下列要求：
(b) 安全政策、安全程序和安全控制；
(c) 安全事件管理计划；
(d) 安全意识和培训计划（适用于支持本次委托的全体员工）；
(e) 安全变更管理计划（用于促进PTC安全环境在安全变更过程中的稳定性和可靠性）；
(f) 永续经营和灾难恢复计划（包括定期测试）；
(g) 用于识别、评估、应对及实施风险处理的安全风险评估程序；
(h) 如果服务提供商在本次委托中开发和提供软件，那么服务提供商的安全软件开发生命周期应符合行业标准（如开放式Web应用程序安全项目(OWASP)的开放软件保证成熟度模型(SAMM)）。
(i) 如果服务提供商为本次委托提供云服务（包括IaaS、PaaS和SaaS），那么服务提供商的实践应符合CSA CCM标准和SOC2标准。

2. 设计和测试的安全性

PTC将维持：

(a) 合理地确保遵守并实施有效的NIST 800-53安全控制的安全架构；
(b) 保护数据所需的有效防火墙和入侵检测技术的系统；
(c) 规定数据隔离的适当网络安全设计元素；
(d) 有关在传输和存储过程中对信息进行加密的程序；
(e) 确保定期测试PTC的安全系统和过程的程序；
(f) 数据库和应用层的设计过程，确保通过设计网站应用程序，保护通过所述系统收集、处理和传输的客户数据。

3. 监测和补丁管理

PTC已经制定并（在相关协议有效期内）维持：

(a) 保持安全补丁最新的机制；
(b) 用于检测对客户数据的试图或实际攻击或入侵的监测系统和程序；
(c) 监测、分析及响应安全警报的程序；
(d) 最先进的商业杀毒软件和反恶意软件的使用和定期更新；以及
(e) 定期验证已安装软件完整性的程序。

4. **PTC**授权用户的远程访问控制

PTC将强制执行：

(a) 适当的机制，以依据“按需知密”的方针进行用户认证和用户授权；
(b) 相关控制措施，对有权远程访问的用户（包括PTC和分处理方（若适用））实施严格的访问限制；
(c) 授权用户账户和认证的及时而准确管理；
(d) 所有密码的加密或散列机制；
(e) 立即撤销不活跃账户/已终止的授权用户/已转移的授权用户的访问权程序；
(f) 确保分工明确的程序；
(g) 确保各个有计算机访问权的授权用户分配唯一ID的程序；
(h) 更改和妥善管理PTC提供的密码和安全参数默认值的规程；以及
(i) 多因素认证对系统（与客户工作说明有关）的合理应用。

5. 设施访问控制

PTC已经制定并（在相关协议有效期内）实施：

(a) 所有信息资产和信息技术的物理保护机制，确保所述资产和信息在适当的数据中心得到储存和保护；
(b) 适当的设施访问控制，限制对系统的物理访问；
(c) 相关规程，确保依据“按需知密”的方针访问设施，并对此进行监督。
(d) 相关措施，防止客户数据和客户依赖的系统因潜在的环境危害（例如火灾、水灾或技术故障）而被破坏、丢失或损坏；以及
(e) 相关控制措施，对所有客户敏感信息进行物理保护，并在不需要客户敏感信息时，妥善销毁所述信息。

[有关PTC网络安全和隐私计划的更多内容，请参阅PTC信任中心 https://www.ptc.com/en/about/trust-center，网站中可以获取PTC ISO27001 和 SOC2 类型 II 的报告。]

附件三
《标准合同条款》

《标准合同条款》的下列模块应适用于 PTC Inc.（作为数据输入方）和客户（包括代表其关联方和其他传输相关控制方作为控制方的客户，若适用）（作为数据输出方），由双方订立，并通过引用方式纳入本附录。

模块 1——从控制方到控制方的传输，其中，客户为控制方；PTC 为独立控制方，负责依据本附录处理个人信息；
模块 2——从控制方到处理方的传输，即将个人传输至 PTC（处理方）；以及
模块 3——从处理方到处理方的传输（其中客户是处理方，PTC 是分处理方）。

就《标准合同条款》而言，下列规定应适用：

- 第 9 条——分处理方的使用。
  - 模块 2 和模块 3
    - 选项 2：一般书面授权；
    - 数据输入方打算通过新增或更换分处理方的方式变更上述名单时，应至少提前 30 天以书面形式通知数据输出方，以便数据输出方在聘用相关分处理方之前拥有足够的时间对名单的变更提出异议。
- 第 17 条——管辖法律
  - 模块 1、模块 2 和模块 3
    - 选项 1；
    - 本附录条款应受欧盟任一成员国的法律管辖，但前提是所述法律支持第三方受益人权利。双方同意：本附录条款应受爱尔兰共和国的法律管辖。
- 第 18 条——法院和司法管辖区的选择
  - 模块 1、模块 2 和模块 3
  - (b) 双方同意：任何争议均应提交至爱尔兰共和国的法院进行裁决。

《标准合同条款》的附件一

A. 缔约方名单
- 1 - 数据输出方：客户，代表其自身或位于欧盟、英国和瑞士的控制方。
- 2 - 数据输入方：PTC，地址是：121 Seaport Boulevard, Boston, MA 02021。
  以及相关协议中客户和 PTC 各自的联系人。

B. 传输说明
个人数据被转移的数据主体的类别

- 模块 1——从控制方到控制方：
  - 经客户授权使用 PTC 产品和/或获取 PTC 服务的个人，包括客户的员工、顾问、分包商、供应商、业务合作伙伴和客户。
- 模块 2——从控制方到处理方
- 客户的员工、顾问、分包商、供应商、业务合作伙伴和客户。客户可能将其个人数据上传到服务项目的其他个人。模块 3——从处理方到处理方
  - 客户的员工、顾问、分包商、供应商、业务合作伙伴和客户。客户可能将其个人数据上传到服务项目的其他个人。

个人数据被转移的数据主体的类别：
传输的个人数据涉及下述类别的数据：

- 模块 1：

姓名、公司、用户名、用户 ID、组织、业务联系人详情、与 PTC 产品和服务的互动（如日志文件和事件报告）。IP 地址、cookie 数据、设备标识符和类似的设备相关信息。

- 模块 2 和模块 3：姓名、公司、组织、业务联系人详情、与 PTC 产品和服务的互动（如日志文件和事件报告），以及上传到 PTC 服务项目的个人数据。敏感数据不得传输。

传输频率（例如，数据是一次性传输还是连续传输）。

数据应连续传输。

处理的性质

数据输入方应按规定处理个人数据，以根据相关协议详细规定的条款和相关协议授权的条款（包括本附录）提供服务。所述处理应包括：

数据输入方提供服务可能需要进行的收集、记录、组织、结构化、存储、改编或更改、检索、咨询、通过传输披露、传播或以其他方式提供、限制、删除或毁坏。

个人数据的保留期限，如果没有保留期限，则需指定用于确定该保留期限的标准。

服务终止时，应依据相关协议的规定从服务项目中删除个人数据。

对于向（分）处理方传输数据，还需指定处理的标的物、性质和持续时间。

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

C. 主管监管机构

- 应依据第 13 条规定确定主管监管机构。
  - 主管监管机构应为爱尔兰共和国的数据保护委员会。

《标准合同条款的附件二——技术措施和组织措施。

本附录附件二应适用。

英国附录

(a) 依据《英国附录》的表 1，各方的详细资料和主要联系信息载于本附录附件三第 A 款。

(b) 依据《英国附录》的表 2，有关《英国附录》所附的经批准的欧盟《标准合同条款》、模块和选定条款的版本的信息载于本附录附件三第 B 款。

(c) 依据《英国附录》的表 3：

1. 缔约方名单载于本附录附件三第 A 款。
2. 传输说明载于附件三第 B 款（处理性质）。
3. 附件二（技术和组织安全措施）应作为《英国附录》的附件二适用。
4. 分处理方名单载于 https://www.ptc.com/-/media/Files/PDFs/legal-agreements/fy18/PTC-Inc-List-of-Sub-processors.pdf.

(d) 依据《英国附录》的表 4，数据输入方和数据输出方均可依据《英国附录》中的条款终止《英国附录》。

2.5 冲突。如果《标准合同条款》或《英国附录》与本 DPA，或本附录中的任何其他条款之间出现任何冲突或不一致，则以《标准合同条款》或《英国附录》中的规定（若适用）为准。