



PTC網路安全和資料隱私附錄(DPA)

本附錄構成客戶與PTC所簽訂相關協議（定義見“相關協議”）的一部分。客戶在適用法律規定的範圍內，代表自身及其關聯方並以關聯方的名義訂立本附錄。在本附錄中，除非另有說明，“客戶”一詞應包括客戶及其關聯方。本附錄中未定義的所有大寫字母術語應具有相關協定規定的含義。

1. 目的與範圍

雙方約定，本附錄是相關協議條款的補充，適用於PTC代表客戶對客戶資料（包括個人資訊）進行的所有處理活動。相關協議條款與本附錄條款發生衝突時，應以本附錄條款為準。

2. 定義

- 2.1. **相關協議**：指PTC與客戶之間簽訂的任何協定，包括但不限於《PTC雲/SaaS服務協定》、《PTC客戶協定（授權合約）》、《全球服務協定》等。PTC根據相關協定向客戶提供服務。
- 2.2. **適用法律**：指GDPR、UK GDPR、CCPA、LGPD以及涉及個人資訊處理和/或個人隱私權或個人資訊處理權保護的任何其他法律法規。
- 2.3. **CCPA**：指《加州消費者隱私法案》（後經《2020年加州隱私權利法案》修訂）/【《加州民法典》第1798.100條等】以及加利福尼亞州司法部長提供的任何相關法規或指南。
- 2.4. **控制方**：指決定個人資訊處理目的和處理方式的實體。
- 2.5. **客戶資料**：指由客戶提供的與服務相關的電子資料和資訊，但不包括非PTC應用程式資訊，或由PTC代表客戶處理的其他資料和資訊，但不包括客戶帳號資料和客戶使用資料。
- 2.6. **客戶帳戶資料**：指與客戶和PTC合作關係有關的個人資料，包括經PTC授權可查看客戶帳戶及相關開票資訊（包括開票位址）的任何自然人的姓名或聯繫資訊（如電子郵寄地址、電話號碼、職務）。客戶帳戶資料還包括PTC為了管理其與客戶的關係、進行身份驗證或相關法律法規另行規定的需要收集的任何資料。
- 2.7. **客戶使用資料**：指公司收集並處理的與提供服務有關的服務使用資料，包括但不限於：與客戶及其使用者使用服務相關的活動，使用者電腦的配置，與客戶及其使用者使用服務有關的性能指標，用於識別通信來源和目的地的資料、活動日誌，以及用於優化和維護服務性能、調查和防止系統濫用的資料。
- 2.8. **資料洩露**：指影響客戶資料的安全性、保密性、可用性或完整性導致客戶資料遭到非法破壞、丟失、更改、未授權披露或訪問的事件。
- 2.9. **GDPR**：指歐洲議會的《通用資料保護條例》（法規編號：(EU) 2016/679）以及該條例在各個國家的實施情況。
- 2.10. **自然人**：指已識別或可識別的自然人；可識別的自然人指可以直接或間接識別的自然人，具體參考與該自然人相關的識別字或其他相關定義。
- 2.11. **LGPD**：指巴西於2018年8月14日頒佈的第13.709號法律《一般個人資料保護法》（後經2019年7月8日第13.853號法律修訂）。
- 2.12. **個人資訊**：指客戶資料中的直接或間接涉及或關聯（或可合理認為直接或間接涉及或關聯）某一特定自然人的任何資訊。
- 2.13. **處理**：指通過自動或非自動方式對客戶資料進行的任何一個或一組操作，例如：訪問、收集、記錄、整理、結構化、存儲、改編或更改、檢索、諮詢、使用，通過傳輸披露、傳播或以其他方式提供、調整或合併、限制、刪除或銷毀。
- 2.14. **服務**：指協定中定義的任何服務。
- 2.15. **《標準合同條款》**：指歐盟委員會於2021年6月4日發佈的《關於根據歐洲議會和歐洲理事會第(EU)2016/679號條例及其經核准修訂案（所述修訂案旨在旨在規範瑞士的個人資料轉移行為）向第三國傳輸個人資料的標準合同條款的實施決定》。
- 2.16. **英國附錄**：指由英國資訊專員發佈並於2022年3月21日生效的歐盟委員會《標準合同條款》的國際資料傳輸附錄（B1.0版）。



2.17. 英國GDPR：指根據英國2018年《退出歐盟法案》第3章保留在英國法律中的GDPR。

本附錄的解釋不得違背適用法律規定的權利和義務，也不得損害任何自然人的基本權利或自由。

3. 目的限制

PTC應僅根據服務的要求以及本DPA的規定，處理客戶資料。PTC不得：(i) 出售客戶資料；(ii) 出於商業目的保留、使用或披露客戶資料（此處所述商業目的不包括提供服務，亦不包括本附錄所述其他目的）；或(iii) 在違反相關協定的情況下保留、使用或披露客戶資料。PTC不得（亦不得允許任何協力廠商）擁有或主張任何客戶資料的任何留置權、抵押權或其他權益。

4. 處理期限

PTC只應在相關協議（及本附錄）的有效期內處理客戶資料。

5. 處理的安全性

- 5.1 PTC已經制定並（在相關協議有效期內）實施技術措施和組織措施（詳見附件二），以確保客戶資料的安全性並防止客戶資料發生資料洩露事件。PTC在評估安全水準時，已經考慮到了技術水準、實施成本、處理的性質、範圍、背景和目的，以及**涉及的風險**。
- 5.2 PTC應在提供服務的嚴格必要範圍內，僅向其工作人員和分處理方授予客戶資料的訪問權。PTC應確保經授權處理客戶資料的人員已經承諾保密，或同意承擔相應法定保密義務。PTC將定期對有許可權訪問客戶資料的人員提供相關網路安全和資料隱私保護方面的培訓。
- 5.3 在不影響雙方之間任何現有合同協定的情況下，PTC應將所有客戶資料視為嚴格保密資訊，並應將此保密性告知其所有參與處理客戶資料的雇員、代理人和/或核准的分處理方。

6. 審計

- 6.1 PTC應定期接受獨立的協力廠商審計員和/或內部審計員的審計，以確認其保護網路安全和隱私的技術措施和組織措施是否充分。PTC應按客戶的要求：i)向客戶提供審計報告的摘要副本；ii)書面答覆客戶提出的涉及客戶資料處理的所有合理資訊要求，包括回復用於確認PTC是否遵守本附錄和適用法律所必需的資訊安全與審計調查問卷，但客戶每個日曆年內提出此要求的次數不得超過一次。如果PTC已就檔所述的某項服務獲得了ISO 27001認證以及根據SSAE 18編制的服務組織控制報告（“SOC2報告”），PTC同意在相關協議有效期內維持相關認證或標準，或其他適當且相當的替代認證或標準。
- 6.2 依據適用法律規定，僅當客戶有理由認為行使上述第6.1款所述權利無法證明PTC遵守本附錄和適用法律時，客戶及其授權代表方可在相關協議的有效期內進行審計（包括檢查），從而確定PTC是否遵守相關協議的條款。任何此類審計（或檢查）必須在PTC的正常營業時間內進行，並應向PTC提供合理通知。PTC和客戶應商定審計範圍、審計時間和審計期限，以及客戶應負責的費用報銷比例。考慮到PTC或其代表所花費的資源，所有報銷比例均應合理。
- 6.3 依據本附錄第6條，客戶及其獨立檢查員應適時簽訂保密協定，以保護PTC在證明其遵守本附錄和適用法律的過程中所披露和提供的所有資訊的保密性。

7. 資料洩露通知

- 7.1 PTC已經實施控制措施和政策，以便發現和及時應對可能造成資料洩露的事件。PTC應及時確定此類事件的上報調查途徑，確認是否已經真實發生資料洩露，採取用於確定資料洩露根源的合理措施，降低任何可能的不利影響，並防止再次發生同類事件。**倘若發生資料洩露**，PTC應考慮到處理性質和現有資訊，與客戶開展合作並協助其履行適用法律規定的義務。
- 7.2 一旦發生資料洩露，PTC應及時通知客戶。無論任何情況，PTC通知客戶的時間均應在其意識到資料洩露發生後的72小時內。在可能的情況下，該等通知應至少包括：
 - (a) “事件經過”：描述資料洩露的性質、首次發現資料洩露的日期和時間，以及已知的可能後果。
 - (b) “相關資訊”：盡可能說明受影響的客戶資料的性質，以及目前已知的自然人和相關資料記錄的類別和大致數量。



- (c) “當前行動”：PTC為解決資料洩露問題所採取或建議採取的措施，包括降低可能的不利影響。
- (d) “行動建議”：PTC建議客戶為降低資料洩露的影響而採取的行動。
- (e) “更多資訊來源”：指可以獲得資料洩露更多相關資訊的聯絡點詳情。

7.3 倘若無法同時提供上述所有資訊，PTC應在知悉進一步資訊之後毫不遲延地通知客戶。

7.4 除非適用法律有所要求，否則PTC在未事先諮詢並獲得客戶的書面同意（客戶不得無故拒絕同意）的情況下，不得因任何資料洩露事件將客戶的名稱或身份告知給除執法部門、法醫人員、保險公司或法律顧問以外的任何自然人或任何協力廠商。如果資料洩露事件影響到PTC的其他客戶，那麼PTC在不披露客戶身份的情況下可以作出一般性的公開聲明。

8. 個人資訊的處理

8.1 雙方明確約定，個人資訊的處理本身不是服務的主體。然而，雙方確認，不能完全排除PTC在一定程度上收到客戶個人資訊的可能性。因此，鑒於客戶可能向PTC披露個人資訊，本附錄的條款應適用於PTC代表客戶處理個人資訊的行為。對於個人資訊，客戶應：i) 確定處理的法律依據；ii) 確保向自然人提供所有適用的隱私通知；以及iii) 根據適用法律要求獲得任何同意。客戶應採取合理措施，確保個人資訊不包括健康資料、政府核發之身份證、信用卡或支付卡資訊等敏感資訊或適用法律規定的特殊類別資料。附件一詳細描述了個人資訊的處理操作，特別是個人資訊的類別，以及PTC代表客戶處理個人資訊的目的。

8.2 PTC應僅根據客戶的書面指示處理個人資訊。相關協定（包括本附錄）構成了客戶的初始書面指示。PTC應盡合理努力遵循客戶的任何其他指示，但前提是客戶的指示符合適用法律的有關規定，具有技術上的可行性，並且不要求改變服務的執行。倘若發生前述任何例外情況，或PTC因故無法遵循指示，或PTC認為某項指示違反了適用法律，PTC將立即通知客戶（可以使用電子郵件發送通知）。

8.3 PTC還可依據適用法律的相關規定處理個人資訊。在這種情況下，除非適用法律以保護重大公共利益為由禁止PTC對外發送通知，否則PTC應在處理個人資訊之前將相關規定通知客戶。

8.4 客戶應對個人資訊的準確性、品質、合法性以及客戶獲取個人資訊方式承擔全部責任。因此，客戶應確保個人資訊的收集和傳輸符合適用法律的相關規定。特別是，客戶應有處理該等個人資訊的法律依據，並通過妥善方式告知相關自然人其個人資訊已收集並處理。

9. 分處理方的使用

9.1 PTC擁有客戶的一般授權，在履行服務義務過程中，可在絕對必要的情況下，委託分處理方處理個人資訊。客戶批准的分處理方名單參見：<https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions>。PTC打算通過新增或更換分處理方的方式變更上述名單時，應至少提前30天通過書面形式通知客戶，以便客戶在聘用相關分處理方之前擁有足夠的時間對名單的變更提出異議。PTC應向客戶提供必要資訊，確保客戶能夠行使異議權。

9.2 聘用分處理方時，PTC應與之簽訂合同。分處理方在該合同項下的個人資訊處理和網路安全義務實際上應與PTC在本附錄下的義務相同。

9.3 PTC應對分處理方代其履行本附錄項下義務的表現，向客戶承擔全部責任。

10. 個人資訊的國際傳輸

10.1 作為一家全球性公司，PTC可能需要在客戶或自然人所在國以外地區處理個人資訊。所有此類個人資訊的傳輸均應符合適用法律，PTC應確保持續採取相關保障措施，確保自然人的權利可強制執行，也確保自然人可以獲得有效的法律救濟。

10.2 歐洲經濟區和瑞士的個人資訊。雙方約定，如果客戶將個人資訊從歐洲經濟區或瑞士傳到PTC，無論直接或間接轉移至歐洲經濟區、瑞士以外任何國家或接收方。歐盟委員會（或相關主管機構（適用於瑞士輸出的個人資訊））認為該等國家或接收方無法對個人資訊提供充分的保護，則適



用《標準合同條款》。對於歐洲經濟區輸出的受限於歐盟《標準合同條款》的個人資訊傳輸，歐盟《標準合同條款》應視為根據附件三訂立（並通過引用納入本附錄）和締結的協議。

10.3 若PTC的《約束性公司規則：處理方政策》適用，則《約束性公司規則：處理方政策》應視為通過引用方式納入本附錄，並且整體上如同本附錄一樣，對客戶具有約束力和可執行性。若《約束性公司規則：處理方政策》與本附錄之間存在任何衝突或不一致，則應以《約束性公司規則：處理方政策》為準。

優先順序。若客戶與PTC之間適用多種傳輸機制，則個人資訊的傳輸將按照下列優先順序適用單一傳輸機制：(i) 《約束性公司規則：處理方政策》；以及(ii) 《標準合同條款》。

10.4 **英國附錄**：雙方約定，如果客戶將個人資訊從英國傳到PTC，無論直接或間接轉移至英國以外的任何國家或接收方，而英國監管機構或政府機關認為該等國家或接收方無法對個人資訊提供充分的保護，則適用《英國附錄》對於英國輸出的受限於《英國附錄》的個人資訊傳輸，《英國附錄》應視為根據附件三訂立（並通過引用納入本附錄）和締結的協議。

10.5 **其他國際傳輸**：如果PTC可能正在代表成立地位於非歐洲經濟區國家、瑞士或英國的客戶處理個人資訊，那麼PTC應確保相關傳輸符合適用法律。這包括將個人資訊傳輸至已經根據適用法律建立《約束性公司規則》的接收方，或已經簽署相關資料保護機構採用或批准的《標準合同條款》的接收方。

11. 在資料隱私義務方面對客戶的協助

11.1 PTC應將自然人提交的關於行使其在適用法律項下相關權利的任何請求及時通知客戶。除非得到客戶的相關授權，否則PTC本身不得對此類請求作出回應。

11.2 鑒於處理的性質及掌握的資訊，PTC應：a) 協助客戶履行其義務，從而對自然人的行權請求作出回應；b) 助力客戶根據適用的法律，遵守下列義務：

- (a) PTC有義務對個人資訊的處理進行風險評估，並且/或者在某類處理可能導致個人權利和自由面臨高風險時，評估相關處理操作對個人資訊保護的影響；
- (b) 若資料保護影響評估結果表明，在客戶未採取措施降低風險的情況下，處理過程將導致高風險，則PTC有義務在處理個人資訊之前諮詢主管監督機構；
- (c) 若PTC知悉其正在處理的個人資訊不準確或已經過時，則PTC有義務通過及時通知客戶的方式來確保相關個人資訊準確且最新；
- (d) PTC有義務協助客戶確保履行個人資訊處理安全性相關的義務。

12. PTC作為控制方：

客戶確認並同意：就客戶帳戶資料和客戶使用資料而言，PTC是獨立控制方，而非與客戶一起構成共同控制方。作為控制方，PTC將處理客戶帳戶資料和客戶使用資料，以期達到下列目的：(i) 管理與客戶的關係；(ii) 執行公司的核心業務運作，如會計、合規目的、客戶關係管理等；(iii) 監測、調查、預防和檢測欺詐、安全事件和其他濫用服務的行為，並防止客戶和客戶資料遭受損害；(iv) 用於身份驗證；(v) 遵守PTC處理和保留個人資訊的相關適用法律或監管義務；以及(vi) 符合適用法律、本附錄和相關協定的有關規定。作為控制方，PTC還可在適用法律允許的範圍內處理客戶使用資料，從而提供、優化、增強和維護服務（如故障排除、開發創新等），為新產品和新功能的開發提供資訊。PTC作為控制方進行的任何處理操作均應符合PTC的隱私政策，具體參見：<https://www.ptc.com/en/documents/policies/privacy>。

13. CCPA規定

依據CCPA規定，在客戶和PTC之間，客戶是一家“企業”，而PTC則是一家出於商業目的接收個人資訊的“服務提供者”。除非為了依據相關協定向客戶提供服務，或者為了依據相關協定和CCPA達成其他目的，否則PTC不得將個人資訊“出售”或“分享”給任何“協力廠商”，亦不得保留、使用或披露任何個人資訊。上述條款中，“企業”、“服務提供者”、“協力廠商”、“銷售”和“分享”的定義參見CCPA第1798.140條。PTC證明其瞭解本附錄第13條所述的限制，並將遵守該等限制。



14. 違反本附錄和協議終止

任何一方的關聯方在本附錄下的責任應受限於相關協議中關於責任排除和責任限制的規定。針對本附錄項下PTC或其關聯方的任何索賠，只能由作為協定一方的客戶實體提出。無論任何情況，本附錄或任何一方均不得限制或約束任何自然人或任何主管監督機構的權利。

15. 客戶資料的檢索和刪除

相關協定終止或期滿後，客戶可立即按相關協定規定輸出客戶資料；或者，若客戶資料無法輸出時，PTC應將客戶資料歸還給客戶。除非適用法律要求繼續保存客戶資料，否則PTC應在相關協議終止後大約30天內，按照相關協議的條款，刪除所有的客戶資料。在刪除或歸還客戶資料之前，PTC應繼續確保遵守本附錄。

16. 其他

16.1 雙方同意，本附錄應取代雙方此前可能已經簽訂的與服務有關的任何《網路安全和資料隱私附錄》。

16.2 除非適用法律另有要求，否則本附錄應受相關協議所述管轄法律和管轄權條款的管轄，並據其進行解釋。

16.3 本附錄和《標準合同條款》將在PTC根據本附錄第15條刪除客戶資料的同時自動終止。

[以下無正文]

附件一

個人資訊已處理的資料主體類別

客戶可以向服務專案提交個人資訊，其範圍由客戶自行決定和控制，其中可能包括但不限於與下列各類自然人有關的個人資訊：

- 客戶的雇員、代理人、顧問、自由職業者（皆為自然人）；
- 客戶的客戶、潛在客戶、商業夥伴和供應商的雇員或連絡人；
- 經客戶授權可使用服務的使用者；

已處理個人資訊的類別

客戶可以向服務專案提交個人資訊，其範圍由客戶自行決定和控制，其中可能包括但不限於下列各類個人資訊：

- 姓名；
- 職務；
- 職位；
- 工作單位；
- 聯繫資訊（公司、電子郵件、電話、實際業務位址）；
- 身份資訊；

已處理的敏感性資料（如果適用）和適用的限制或保障措施，充分考慮到資料的性質和所涉及的風險，例如，嚴格的目的限制，訪問限制（包括只有經過專門培訓的員工才能訪問），保存資料訪問記錄，限制轉發或其他安全措施。

- 無

處理的性質

- 為提供服務可能需要進行的收集、記錄、組織、結構化、存儲、改編或更改、檢索、諮詢、通過傳輸披露、傳播或以其他方式提供、限制、刪除或毀壞。

代表客戶處理個人資訊的目的

- 提供相關協定具體規定的服務

處理期限

- PTC 根據相關協定提供服務的期限，以及該期限的任何延長期或續期。

技術措施和組織措施（包括旨在確保客戶資料安全性的技術措施和組織措施）

“網路”：指相互連接並可通過局域網（LAN）和廣域網路（WAN）共用資料的電腦、伺服器、主機、網路設備、週邊設備或其他設備的集合。

“安全控制措施”：指依據相關協議的規定，為強制執行NIST 800-53所需的任何具體的硬體、軟體或管理機制，用於應對資訊技術系統和相關物理位置的安全風險或實施相關政策。安全控制措施規定了技術、方法、實施程式和其他詳細因素或其他流程，用於實施與特定群體、個人或技術有關的安全政策要素。

“安全政策”：指確保公司安全相關資訊和確保適用法律法規合規性的方向性聲明。

“安全程式”：指為實現並維持NIST 800-53和/或ISO27001認證而採取的分步行動。

“系統”：指電腦軟體、固件、電腦硬體（無論是通用還是專用）、電信能力（包括所有語音、資料和視頻網路）和/或其他類似或相關的自動化專案、電腦化專案和/或軟體專案。

為了遵守相關協議和本附錄規定的安全義務，PTC應始終：(i)擁有符合ISO27001認證等行業最佳標準的安全程式，或應實施美國國家標準技術研究所(NIST)800-53安全要求的“中等”影響控制措施；(ii)制定本附錄中規定的安全要求、義務、規範和事件報告程式。

1. 安全計畫和治理

PTC應始終維持包含下列內容的安全計畫：

- (a) 首席資訊安全官或安全指定人員，負責管理下列要求；
- (b) 安全政策、安全程式和安全控制；
- (c) 安全事件管理計畫；
- (d) 安全意識和培訓計畫（適用於支持本次委託的全體員工）；
- (e) 安全變更管理計畫（用於促進PTC安全環境在安全變更過程中的穩定性和可靠性）；
- (f) 永續經營和災難恢復計畫（包括定期測試）；
- (g) 用於識別、評估、應對及實施風險處理的安全風險評估程式；
- (h) 如果服務提供者在本次委託中開發和提供軟體，那麼服務提供者的安全軟體發展生命週期應符合行業標準（如開放式Web應用程式安全專案(OWASP)的開放軟體保證成熟度模型(SAMM)）。
- (i) 如果服務提供者為本次委託提供雲服務（包括IaaS、PaaS和SaaS），那麼服務提供者的實踐應符合CSA CCM標準和SOC2標準。

2. 設計和測試的安全性

PTC將維持：

- (a) 合理地確保遵守並實施有效的NIST 800-53安全控制的安全架構；
- (b) 保護資料所需的有效防火牆和入侵偵測技術的系統；
- (c) 規定資料隔離的適當網路安全設計項目；
- (d) 有關在傳輸和存儲過程中對資料進行加密的程式；
- (e) 確保定期測試PTC的安全系統和過程的程式；
- (f) 資料庫和應用層的設計過程，確保通過設計網站應用程式，保護通過所述系統收集、處理和傳輸的客戶資料。

3. 監測和補丁管理

PTC已經制定並（在相關協議有效期內）維持：

- (a) 保持安全補丁最新的機制；
- (b) 用於檢測對客戶資料的試圖或實際攻擊或入侵的監測系統和程式；
- (c) 監測、分析及回應安全警報的程式；
- (d) 最先進的商業殺毒軟體和反惡意軟體的使用和定期更新；以及
- (e) 定期驗證已安裝軟體完整性的程式。

4. PTC授權使用者的遠端存取控制

PTC將強制執行：

- (a) 適當的機制，以依據“按需知密”的方針進行用戶認證和用戶授權；
- (b) 相關控制措施，對有權遠端存取的用戶（包括PTC和分處理方（若適用））實施嚴格的訪問限制；
- (c) 授權使用者帳戶和認證的及時而準確管理；
- (d) 所有密碼的加密或散列機制；
- (e) 立即撤銷不活躍帳戶/已終止的授權使用者/已轉移的授權使用者的訪問權程式；
- (f) 確保分工明確的程式；
- (g) 確保各個有電腦訪問權的授權使用者分配唯一ID的程式；
- (h) 更改和妥善管理PTC提供的密碼和安全參數預設值的規程；以及
- (i) 多因素認證對系統（與客戶工作說明有關）的合理應用。

5. 設施存取控制

PTC已經制定並（在相關協議有效期內）實施：

- (a) 所有資訊資產和資訊技術的物理保護機制，確保所述資產和資訊在適當的資料中心得到儲存和保護；
- (b) 適當的設施存取控制，限制對系統的物理訪問；
- (c) 相關規程，確保依據“按需知密”的方針訪問設施，並對此進行監督。
- (d) 相關措施，防止客戶資料和客戶依賴的系統因潛在的環境危害（例如火災、水災或技術故障）而被破壞、丟失或損壞；以及
- (e) 相關控制措施，對所有客戶敏感資訊進行物理保護，並在不需要客戶敏感資訊時，妥善銷毀所述資訊。

[有關 PTC 網路安全和隱私計畫的更多內容，請參閱 PTC 信任中心 <https://www.ptc.com/en/about/trust-center>，網站中可以獲取PTC ISO27001 和 SOC2 類型 II 的報告。]

附件三
《標準合同條款》

《標準合同條款》的下列模組應適用於 PTC Inc.（作為資料登錄方）和客戶（包括代表其關聯方和其他傳輸相關控制方作為控制方的客戶，若適用）（作為資料輸出方），由雙方訂立，並通過引用方式納入本附錄。

模組 1——從控制方到控制方的傳輸，其中，客戶為控制方；PTC 為獨立控制方，負責依據本附錄處理個人資訊；

模組 2——從控制方到處理方的傳輸，即將個人傳輸至 PTC（處理方）；以及

模組 3——從處理方到處理方的傳輸（其中客戶是處理方，PTC 是分處理方）。

就《標準合同條款》而言，下列規定應適用：

- 第 9 條——分處理方的使用。
 - 模組 2 和模組 3
 - 選項 2：一般書面授權；
 - 資料登錄方打算通過新增或更換分處理方的方式變更上述名單時，應至少提前 30 天以書面形式通知資料輸出方，以便資料輸出方在聘用相關分處理方之前擁有足夠的時間對名單的變更提出異議。
- 第 17 條——管轄法律
 - 模組 1、模組 2 和模組 3
 - 選項 1；
 - 本附錄條款應受歐盟任一成員國的法律管轄，但前提是所述法律支持協力廠商受益人權利。雙方同意：本附錄條款應受愛爾蘭共和國的法律管轄。
- 第 18 條——法院和司法管轄區的選擇
 - 模組 1、模組 2 和模組 3
 - (b) 雙方同意：任何爭議均應提交至愛爾蘭共和國的法院進行裁決。

《標準合同條款》的附件一

A. 締約方名單

- 1 - 資料輸出方：客戶，代表其自身或位於歐盟、英國和瑞士的控制方。
- 2 - 資料登錄方：PTC，地址是：121 Seaport Boulevard, Boston, MA 02021。
以及相關協定中客戶和 PTC 各自的連絡人。

B. 傳輸說明

個人資料被轉移的資料主體的類別

- 模組 1——從控制方到控制方：
 - 經客戶授權使用 PTC 產品和/或獲取 PTC 服務的個人，包括客戶的員工、顧問、分包商、供應商、業務合作夥伴和客戶。
- 模組 2——從控制方到處理方
- 客戶的員工、顧問、分包商、供應商、業務合作夥伴和客戶。客戶可能將其個人資料上傳到服務專案的其他個人。模組 3——從處理方到處理方
 - 客戶的員工、顧問、分包商、供應商、業務合作夥伴和客戶。客戶可能將其個人資料上傳到服務專案的其他個人。

個人資料被轉移的資料主體的類別：

傳輸的個人資料涉及下述類別的資料：

- 模組 1：

姓名、公司、用戶名、使用者 ID、組織、業務聯絡人詳情、與 PTC 產品和服務的互動（如日誌檔和事件報告）。IP 位址、cookie 資料、設備識別字和類似的設備相關資訊。

- 模組 2 和模組 3：姓名、公司、組織、業務聯絡人詳情、與 PTC 產品和服務的互動（如日誌檔和事件報告），以及上傳到 PTC 服務專案的個人資料。敏感性資料不得傳輸。

傳輸頻率（例如，資料是一次性傳輸還是連續傳輸）。

資料應連續傳輸。

處理的性質

資料登錄方應按規定處理個人資料，以根據相關協定詳細規定的條款和相關協議授權的條款（包括本附錄）提供服務。所述處理應包括：

資料登錄方提供服務可能需要進行的收集、記錄、組織、結構化、存儲、改編或更改、檢索、諮詢、通過傳輸披露、傳播或以其他方式提供、限制、刪除或毀壞。

個人資料的保留期限，如果沒有保留期限，則需指定用於確定該保留期限的標準。

服務終止時，應依據相關協定的規定從服務專案中刪除個人資料。

對於向（分）處理方傳輸資料，還需指定處理的標的物、性質和持續時間。

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

C. 主管監管機構

- 應依據第 13 條規定確定主管監管機構。
 - 主管監管機構應為愛爾蘭共和國的資料保護委員會。

《標準合同條款的附件二——技術措施和組織措施。

本附錄附件二應適用。

(a) 依據《英國附錄》的表 1，各方的詳細資料和主要聯繫資訊載於本附錄附件三第 A 款。

(b) 依據《英國附錄》的表 2，有關《英國附錄》所附的經批准的歐盟《標準合同條款》、模組和選定條款的版本的資訊載於本附錄附件三第 B 款。

(c) 依據《英國附錄》的表 3：

1. 締約方名單載於本附錄附件三第 A 款。
2. 傳輸說明載於附件三第 B 款（處理性質）。
3. 附件二（技術和組織安全措施）應作為《英國附錄》的附件二適用。
4. 分處理方名單載於 <https://www.ptc.com/-/media/Files/PDFs/legal-agreements/fy18/PTC-Inc-List-of-Sub-processors.pdf>。

(d) 依據《英國附錄》的表 4，資料登錄方和資料輸出方均可依據《英國附錄》中的條款終止《英國附錄》。

2.5 衝突。如果《標準合同條款》或《英國附錄》與本 DPA，或本附錄中的任何其他條款之間出現任何衝突或不一致，則以《標準合同條款》或《英國附錄》中的規定（若適用）為準。