PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

SAP 雲端服務個人資料處理合約

1. BACKGROUND

背景

1.1 Purpose.

目的

This document is a data processing agreement ("**DPA**") between SAP and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Cloud Service. It states the technical and organizational measures SAP uses to protect Personal Data that is stored in the production system of the Cloud Service.

本文件係 SAP 與客戶之間訂定之資料處理合約 (以下稱「**DPA**」)，適用於客戶提供之個人資料及其使用雲端服務所相關之所有資料控管者。該文件亦規範 SAP 保護儲存於雲端服務生產系統之個人資料所用的技術及組織措施。

1.2 Application of the Standard Contractual Clauses Document.

標準議約條款文件之適用

If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.

處理涉及國際傳輸之個人資料時，應適用第 5 條所載之標準契約條款並將其納入參考。

1.3 Governance.

管理

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use the Cloud Service to the terms of this DPA.

除第 5.2 條規定外，客戶應全權負責管理其他資料控管者所提出之請求。客戶應要求其允許使用雲端服務之任何其他資料控管者遵守本 DPA 之規定。

2. APPENDICES

附錄

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in the Cloud Service. Appendix 1 states the details of the processing SAP will provide via the Cloud Service. Appendix 2 states the technical and organizational measures SAP applies to the Cloud Service, unless the Agreement states otherwise.

客戶及其資料控管者應確定收集及處理本雲端服務中的個人資料的目的。附錄 1 規範 SAP 應透過雲端服務提供之詳細處理資訊。除非本合約另有說明，否則附錄 2 應規範 SAP 用於雲端服務之技術及組織措施。

3. SAP OBLIGATIONS

SAP 義務

3.1 Instructions from Customer.

客戶指示

SAP will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Cloud Service. SAP may correct or remove any Personal Data in accordance with the Customer's instruction. If SAP cannot comply with an instruction, it will promptly notify Customer (email permitted).

SAP 對於個人資料應 (代表自身或其資料控管者) 依循客戶之指示，除非該資料：(i) 依法禁止；或 (ii) 需對雲端服務

進行重大變更。SAP 得依客戶指示更正或移除任何個人資料。如 SAP 無法依循指示，其應立即通知客戶 (得以電子郵件)。

3.2 Data Secrecy.

資料保密

To process Personal Data, SAP and its Subprocessors will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law. SAP and its Subprocessors will regularly train individuals having access to Personal Data in data security and data privacy measures.

針對個人資料之處理，SAP 及其分包處理商僅應聘用依資料保護法而有義務遵守資料保密及電信保密之人員。SAP 及其分包處理商應對可存取個人資料之員工，定期舉行關於資料保密與資料隱私之訓練。

3.3 Technical and Organizational Measures.

技術和組織措施

(a) SAP will use the appropriate technical and organizational measures stated in Appendix 2.

SAP 應使用附錄 2 所載之適當技術及組織措施。

(b) Appendix 2 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.

附錄 2 適用於雲端服務生產系統。客戶不得將任何個人資料儲存於非正式運作環境中。

(c) SAP provides the Cloud Service to SAP's entire customer base hosted out of the same data center and receiving the same Cloud Service. Customer agrees SAP may improve the measures taken in Appendix 2 in protecting Personal Data so long as it does not diminish the level of data protection.

SAP 應提供雲端服務予託管在相同資料中心以外並享有相同雲端服務之整體客戶群。客戶同意 SAP 得在不降低資料保護層級之情況下，改善附錄 2 中為保護個人資料所採取之措施。

3.4 Security Breach Notification.

安全性違反通知

SAP will promptly inform Customer if it becomes aware of any Security Breach.

一旦 SAP 察覺任何違反安全性之狀況，應立即通知客戶。

3.5 Cooperation.

合作

At Customer's request, SAP will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data.

應客戶之請求，凡資料主體或監管機關要求 SAP 處理個人資料，SAP 應合理協助客戶或任何資料控管者處理。

4. SUBPROCESSORS

分處理商

4.1 Permitted Use.

許可的用途

(a) Customer and Data Controllers authorize SAP to subcontract the processing of Personal Data to Subprocessors. SAP is responsible for any breaches of the Agreement caused by its Subprocessors.

客戶及資料控管者授權 SAP 將個人資料處理轉包給分包處理商。SAP 應擔負其分包處理商違約之責。

(b) Subprocessors will have the same obligations as SAP does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.

分包處理商處理個人資料所應履行之義務，與 SAP 擔任資料處理者 (或分包處理商) 時相同。

(c) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, SAP will regularly evaluate each Subprocessor's security practices as they relate to data handling.

SAP 應先評估分包處理商對安全性、隱私性以及機密性之實踐，再進行選擇。分包處理商得具備安全性認證，以證明其使用適當之安全措施。若無，則 SAP 應定期評估各分包處理商處理資料時，對安全性之實踐。

(d) If Customer requests, SAP will inform Customer of the name, address and role of each Subprocessor it uses to provide the Cloud Service.

經客戶要求後，SAP 應告知客戶每位其藉以提供本雲端服務之分包處理商的名稱、地址與角色。

4.2 New Subprocessors.

新分處理商

SAP's use of Subprocessors is at its discretion, provided that:

有下列情形者，SAP 得自行決定對分包處理商之聘用：

(a) SAP will notify Customer in advance (by email or by posting on the Support Portal) of any changes to the list of Subprocessors in place on the Effective Date (except for Emergency Replacements or deletions of Subprocessors without replacement).

SAP 就分包處理商名單之任何變動，應於生效日 (以電子郵件或公佈於 Support Portal 之方式) 事先通知客戶。

(b) If Customer has a legitimate reason that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within thirty days after receipt of SAP's notice. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor.

有關分包處理商對個人資料之處理，只要客戶具備合法理由，便可於收到 SAP 通知後三十日內，以書面通知反對 SAP 聘用分包處理商。若客戶反對聘用分包處理商，雙方應本於誠信原則共商解決方案。SAP 得選擇：(i) 不聘用分包處理商；或 (ii) 履行客戶於反對事由中所要求之修正步驟，再聘用分包處理商。若上開選項皆無法合理履行，且客戶基於合法理由持續反對，當事人任一方便得於三十日內以書面通知終止本合約。若客戶未於收到通知後三十日內表達反對意見，則視為客戶接受新分包處理商。

(c) If Customer's objection remains unresolved sixty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to accept the Subprocessor.

若客戶之反對事由於提出後六十日內仍未獲解決，且 SAP 未收到任何終止通知，則視為客戶接受分包處理商。

4.3 Emergency Replacement.

緊急更換

SAP may change a Subprocessor where the reason for the change is outside of SAP's reasonable control. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).

SAP 得替換分包處理商，且該替換事由非 SAP 可合理控制。在此情況下，SAP 應立即通知客戶該分包處理商之替換。依第 4.2(b) 之規定，客戶保留反對替換分包處理商之權利。

5. INTERNATIONAL TRANSFERS

國際傳輸

5.1 Limitations on International Transfer.

國際傳輸限制

Personal Data from an EEA or Swiss Data Controller(s) may only be exported or accessed by SAP or its Subprocessors outside the EEA or Switzerland (**"International Transfer"**):

EEA 或瑞士資料控管者之個人資料僅得由 SAP 或其位於 EEA 或瑞士境外之分包處理商加以匯出或存取（以下稱**「國際傳輸」**）：

(a) If the recipient, or the country or territory in which it processes or accesses Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission; or

有關個人資料之處理，若接收者或其處理或存取個人資料所在之國家/地區或領域可提供有歐洲執行委員會決定之對資料主體權利與自由的適當水準保護；或

(b) in accordance with Section 5.2.

依第 5.2 條之規定。

5.2 Standard Contractual Clauses and Multi-tier Framework.

標準契約條款及多層架構

(a) The Standard Contractual Clauses apply where there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission.

有關個人資料之處理，若國家/地區之國際傳輸無法提供有歐洲執行委員會決定之對資料主體權利與自由的適當水準保護，則適用本標準契約條款。

(b) For Third Country Subprocessors, SAP has entered into the unchanged version of the Standard Contractual Clauses prior to the Subprocessor's processing of Personal Data. Customer hereby (itself as well as on behalf of each Data Controller) accedes to the Standard Contractual Clauses between SAP and the Third Country Subprocessor. SAP will enforce the Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller if a direct enforcement right is not available under Data Protection Law.

對於第三國分包處理商，SAP 已於該分包處理商處理個人資料前，先行簽訂標準契約條款的原始版本。客戶（本身及代表各資料控管者）特此同意 SAP 與第三國分包處理商之間訂定之標準契約條款。若依資料保護法律無法直接履行權利，則 SAP 應代表資料控管者對分包處理商履行該標準契約條款。

(c) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

本 DPA 中任何規定不得解釋為優先於標準契約條款的任何衝突條款。

6. CERTIFICATIONS AND AUDITS

認證及稽核

6.1 Customer Audits.

客戶稽核

Customer or its independent third party auditor may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

在下列情況下，客戶或其獨立第三方稽核員得稽核 SAP 處理個人資料的相關控制環境與安全性做法：

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 attestation report. Upon Customer's request -SOC Audit reports or ISO certifications are available through the third party auditor or SAP;

SAP 未提出下列充分證據，證明已履行可保護雲端服務生產系統之技術及組織措施：(i) 符合 ISO 27001 或其他標準之認證 (認證範圍如憑證所定義)；或 (ii) 有效之 ISAE3402 和/或 ISAE3000 鑑定報告。於客戶要求時，透過第三方稽核員或 SAP 提供 SOC 稽核報告或 ISO 認證；

(b) A Security Breach has occurred;

發生違反安全性之狀況；

(c) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this DPA;

客戶或其他資料控管者有合理理由足以認為 SAP 未依本 DPA 履行其義務；

(d) An audit is formally requested by Customer's or another Data Controller's data protection authority; or

稽核請求係由客戶或其他資料控管者的資料保護主管機關所正式提出；或

(e) Mandatory Data Protection Law provides Customer with a direct audit right.

強制性資料保護法授予客戶直接稽核權利。

Where Customer audits SAP's environment, SAP will reasonably support Customer in its audit processes.

客戶稽核 SAP 環境時，SAP 應於稽核程序中向客戶提供合理支援。

6.2 Audit Restrictions.

稽核限制

The Customer audit will be limited to once in any twelve month period, and limited in time to a maximum of 3 business days and scope as reasonably agreed in advance between the parties. Reasonable advance notice of at least sixty days is required, unless Data Protection Law requires earlier audit. SAP and Customer will use current certifications or other audit reports to minimize repetitive audits. Customer and SAP will each bear their own expenses of audit, unless the Customer is auditing under Section 6.1 (c) (unless such audit reveals a breach by SAP in which case SAP shall bear its own expenses of audit), 6.1 (d) or 6.1 (e). In those cases, Customer will bear its own expense and the cost of SAP's internal resources required to conduct the audit. If an audit determines that SAP has breached its obligations under the Agreement, SAP will promptly remedy the breach at its own cost.

客戶稽核之頻率應限制為十二個月一次，時間亦應限制為至多 3 個工作日，範圍則事先經雙方合理同意。除資料保護法規定需提前稽核外，理應於六十日內事先通知。SAP 及客戶應使用目前認證或其他稽核報告，盡可能減少重複性稽核。除客戶依第 6.1 (c) (經是類稽核發現 SAP 有任何違規情形而應承擔其稽核費用者，不在此限)、6.1 (d) 或 6.1

(e) 條規定進行稽核之情形外，客戶及 SAP 應各自負擔稽核費用。在前開情況下，客戶應負擔其本身之費用及 SAP 執行稽核所需內部資源的成本。若稽核判定 SAP 違反本合約所規定之義務，SAP 應立即自費予以補救。

7. EU ACCESS
EU ACCESS

7.1 Optional Service.
選購服務

If included in the Order Form, SAP agrees to provide EU Access for the eligible Cloud Service as stated in this Section 7.

若包含於本訂購單中，SAP 同意依第 7 條所載規定向符合資格的雲端服務提供 EU Access。

7.2 EU Access.
EU Access

SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service.

SAP 應僅聘用歐洲分包處理商，以提供需要雲端服務中個人資料存取權的支援。

7.3 Data Center Location.
資料中心地點

Upon the Order Form Effective Date, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a data center within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

自訂購單生效日起，用於代管雲端服務中個人資料的資料中心均位於 EAA 或瑞士。未經客戶事先書面同意 (允許使用電子郵件)，SAP 不得將客戶執行個體移轉至位在 EEA 或瑞士以外的資料中心。若 SAP 計畫將客戶執行個體移轉至位在 EEA 或瑞士的資料中心，SAP 應在預計移轉的三十日前以書面 (允許使用電子郵件) 通知客戶。

7.4 Exclusions.
例外狀況

The following Personal Data is not subject to the requirements in 7.2-7.3:

下列個人資料不受第 7.2-7.3 條所載需求之約束：

(a) Contact details of the sender of a support ticket;

支援單傳送者的聯絡人詳細資料；

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP;

客戶在發出支援單時，所提交的其他個人資料。客戶得選擇在發出支援單時，不傳送個人資料。若事故管理程序需要該資料，則客戶傳送事故訊息給 SAP 前，得選擇先將該個人資料匿名處理。

(c) Personal Data in non-production systems.

非生產系統中的個人資料。

8. DEFINITIONS
名詞定義

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

本文中未定義之英文大寫詞彙，其含義應與合約中相同。

8.1 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at**:** http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

「資料中心」係指於客戶區域內為其代管雲端服務生產執行個體之所在地，其位置已公布於下列網址、事先通知客戶或另定於訂購單中：http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html。

8.2 **"Data Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

「資料控管者」係指自然人或法人、公共機構、機構或其他機關，而其單獨或與他人共同負責決定個人資料處理之目的與方法。

8.3 **"Data Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

「資料處理者」係指代表控管者處理個人資料之自然人或法人、公共機構、機構或其他機關。

8.4 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

「資料保護法」係指保護個人基本權利和自由，以及依本合約處理個人資料時相關隱私權的法律。

8.5 **"Data Subject"** means an identified or identifiable natural person.

「資料主體」係指已列載或可識別之自然人。

8.6 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

「EEA」係指歐洲經濟區，亦即歐盟會員國及冰島、列支敦士登和挪威。

8.7 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

「歐洲分包處理商」係指位於 EEA 或瑞士，對個人資料進行實際處理的分包處理商。

8.8 **"Personal Data"** means any information relating to a Data Subject For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service. It also includes personal data supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data.

「個人資料」係指基於本 DPA 之目的，與資料主體有關的任何資訊，其僅包含由客戶或其授權使用者輸入或於使用雲端服務時所產生之個人資料。該資料亦包含 SAP 或其分包處理商為依本合約提供支援所取得或存取之個人資料。個人資料係客戶資料子集。

8.9 **"Security Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

「安全性違反」係指下列經過確認之情形：(1) 客戶個人資料或機密資料遭意外或非法損毀、遺失、竄改或揭露；或 (2) 涉及個人資料之類似事件，依適用法律規定，資料處理者應將是類事件通知資料控管者。

8.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. They include

Appendices 1 and 2 attached to this DPA.

「**標準契約條款**」(有時亦稱為「EU 示範條款」) 係指 (標準契約條款 (處理商)) 或任何執委會發布之後續版本 (其應自動適用)。現行標準契約條款位於下列網址：http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc。該條款包含本 DPA 附加之附錄 1 和 2。

8.11 "Subprocessor" means SAP Affiliates and third parties engaged by SAP or SAP's Affiliates to process personal data.

「**分包處理商**」係指可處理個人資料之 SAP 關係企業以及與 SAP 或其關係企業訂約的第三方。

8.12 "Third Country Subprocessor" means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

「**第三國分包處理商**」係指 EEA 以外與歐洲委員會已發佈正式認可之任何國家/地區以外的任何分包處理商，其已公佈於下列網址：http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm。

Appendix 1 to Data processing agreement and Standard Contractual Clauses
資料處理合約與標準契約條款的附錄 1

Data Exporter
資料匯出者

The Data Exporter subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.

訂閱雲端服務之資料匯出者，該服務允許其授權使用者輸入、修訂、使用、刪除或以其他方式處理個人資料。

Data Importer
資料匯入者

SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP 及其分包處理商所提供的雲端服務包含下列支援：

SAP Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

SAP 關係企業均以 SAP 設施為基地提供對雲端服務資料中心的遠端支援，該設施位於位於聖里昂/熱特 (德國)、印度及其他負責營運/雲端遞送功能之 SAP 聘雇人員所在地點。支援包含：

- Monitoring the Cloud Service
  監控雲端服務
- Backup & restoration of Customer Data stored in the Cloud Service
  備份與還原儲存於雲端服務中的客戶資料
- Release and development of fixes and upgrades to the Cloud Service
  發行與開發雲端服務之修復與更新程式
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
  監控、疑難排解與管理基礎雲端服務架構及資料庫
- Security monitoring, network-based intrusion detection support, penetration testing
  安全性監控、網際網路型入侵偵測支援、滲透測試

SAP Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

當客戶因雲端服務無法使用或無法如部分或所有授權使用者預期般運作，而提交支援請求單時，SAP 關係企業將提供支援。SAP 會接聽電話並執行基本疑難排解，同時於追蹤系統中處理支援請求單，該系統獨立於雲端服務的生產執行個體之外。

Data Subjects
資料主體

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of data subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

除非資料匯出者另行提供，否則傳輸之個人資料將涉及下列類別的資料主體：員工、承包商、業務夥伴或其他擁有雲端服務所存個人資料的個人。

Data Categories

資料類別

The transferred Personal Data transferred concerns the following categories of data:

傳輸之個人資料涉及下列類別之資料：

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

客戶根據所訂閱之雲端服務決定資料類別。客戶得於雲端服務建置期間設定資料欄位，或採取雲端服務另行提供之方式。傳輸之個人資料通常涉及下列類別之資料：姓名、電話號碼、電子郵件地址、時區、地址資料、系統存取/使用/授權資料、公司名稱、契約資料、帳單資料，以及授權使用者訂立本雲端服務之任何應用特定資料，其得包括銀行帳戶資料、信用卡或簽帳卡資料。

Special Data Categories (if appropriate)

特殊資料類別 (若適用)

The transferred Personal Data concerns the following special categories of data: As set out in the Order Form, if any.

傳輸之個人資料涉及下列特殊的資料類別：如訂購單所規範 (如有)。

Processing Operations

處理操作

The transferred Personal Data is subject to the following basic processing activities:

傳輸之個人資料受下列基本處理作業所規範：

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
  使用個人資料來設定、執行、監控及提供雲端服務 (包括營運與技術支援)
- provision of Consulting Services;
  提供諮詢服務；
- communication to Authorized Users
  與授權使用者進行溝通
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
  在專用服務資料中心 (多組織用戶架構) 儲存個人資料
- upload any fixes or upgrades to the Cloud Service
  將修補或更新程式上傳至雲端服務
- back up of Personal Data
  個人資料備份
- computer processing of Personal Data, including data transmission, data retrieval, data access
  電腦處理個人資料，包括資料傳輸、資料擷取、資料存取
- network access to allow Personal Data transfer
  允許傳輸個人資料的網路存取權
- execution of instructions of Customer in accordance with this Agreement
  依據本合約履行客戶指示

Appendix 2 – Technical and Organizational Measures
附錄 2 – 技術及組織措施

1. TECHNICAL AND ORGANIZATIONAL MEASURES
技術和組織措施

The following sections define the SAP's current security measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

以下各條定義 SAP 目前的安全措施。SAP 得於維持同等或更佳安全水準時，隨時不為通知變更這些措施。此意味個別措施可由具備相同用途而不降低安全水準之新措施取代。

1.1 Physical Access Control.
實體存取控制

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

應禁止未經授權人員對可處理及/或使用個人資料之資料處理系統所在的場所、大樓或房間取得實體進出權。

Measures

措施：

- SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

  SAP 採用適當方式根據內部安全部門開展的安全分類保護其資產與設施。

- In general, buildings are secured through access control systems (e.g., smart card access system).

  通常，建築係透過存取控制系統取得保護 (例如：智慧卡存取系統)。

- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

  作為最低要求，建築最外圍入口點必須配備經認證之金鑰系統，包括現代、活躍的金鑰管理。

- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.

  根據安全分類，建築、個人區域及周圍住所得由其他措施保護。這些措施包括特定存取設定檔、監視錄影、入侵者報警系統以及包括生物計量之存取控制系統。

- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.

  存取權將依系統與資料存取控制措施 (參照下述第 1.2 及 1.3 條) 個別授予經授權之人。這也適用於訪客進出。SAP 建築之來賓與訪客必須於接待處登記姓名，並由經授權之 SAP 人員陪同。

- SAP employees and external personnel must wear their ID cards at all SAP locations.

  SAP 員工和外部人員在 SAP 所有地點必須配戴身分牌。

Additional measures for Data Centers:

資料中心之其他措施：

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized

representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

所有資料中心遵守嚴格之安全程序，其由守衛、 監視照相機、運動檢測器、存取控制機制及其他防止未完全遵守該安全程序之設備與資料中心設施所執行。僅經授權之代表方可使用資料中心內之系統與設備。為確保適當之功能，實體安全設備 (例如：運動檢測器、相機等) 應定期維修。

- SAP and all third party Data Center providers log the names and times of persons entering SAP's private areas within the Data Centers.

  SAP 與所有第三方資料中心提供者均記錄進入資料中心內 SAP 私領域之人員姓名與進入時間。

1.2 System Access Control.

系統存取控制

Data processing systems used to provide the SAP Services must be prevented from being used without authorization.

應防止提供 SAP 服務之資料處理系統未經授權而被使用。

Measures:

措施：

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.

  授予包括個人資料之儲存與處理的敏感系統使用途徑時，將使用不同授權等級。處理程序已佈置就緒，可確保授權使用者具備新增、刪除或修改使用者之相關權限。

- All users access SAP's systems with a unique identifier (user ID).

  所有使用者皆使用唯一識別碼 (使用者 ID) 存取 SAP 系統。

- SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.

  SAP 已將程序佈置就緒，以確保請求之授權變更僅根據指南 (例如，需授權才能授予權利) 得以實作。如果使用者離開公司，其存取權將被撤銷。

- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

  SAP 制定了密碼政策，其禁止共用密碼、管制密碼遭揭露之因應作為以及要求定期變更密碼，且預設密碼應被更換。個人化使用者 ID 被分配用於驗證。所有密碼應符合規定之最低要求，並以加密方式儲存。在使用網域密碼的情況下，系統依照密碼難度之要求，強制每六個月變更一次密碼。每台電腦皆有受密碼保護之螢幕保護程式。

- The company network is protected from the public network by firewalls.

  公司網路透過防火牆不受公共網路之害。

- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

  SAP 於公司網路 (適用於電子郵件帳戶) 之存取點、所有檔案伺服器以及所有工作站上使用最新之防毒軟體。

- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.

  採用安全性補綴程式管理以確保相關安全性更新之 常態與定期部署。
- Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

  全部 SAP 公司之網路及重要設施之遠端途徑經 嚴格驗證受到保護。

1.3 Data Access Control .

資料存取控制

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

有權使用資料處理系統之個人將僅對其有權存取之個人資料進行存取，並且在處理、使用、儲存過程中，未經授權不得閱讀、複製、修改或移除個人資料。

Measures:

措施：

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

  作為 SAP 安全性政策之一部分，個人資料之保護程度至少應達 SAP 資訊分級標準規定之「機密」資訊等級。
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards. Confidential information must be processed confidentially.

  在「有知情需要」的基礎上授予個人、保密或敏感資訊的存取權限。換言之，員工或外部第三方可以存取所需資訊以便完成工作。SAP 使用記錄了如何指定授權及為其指定哪些授權的授權概念。所有個人、機密或其他敏感資料皆依 SAP 之安全政策與標準受到保護。保密資訊必須進行保密處理。
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.

  所有生產伺服器皆於資料中心或安全無虞之伺服器機房中運作。保護處理個人、機密或其他敏感資訊之應用程式之安全措施接受定期檢查。有鑑於此，SAP 於其 IT 系統上進行內外部安全檢查和滲透測試。
- SAP does not allow the installation of personal software or other software that has not been approved by SAP.

  SAP 不允許安裝未獲 SAP 核准之個人軟體或其他軟體。
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

  SAP 安全標準可管制如何刪除或銷毀不再需要的資料及資料載體。

1.4 Data Transmission Control.

資料傳輸控制

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented

at SAP to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).
除了根據相關服務合約提供服務需要資料傳輸控制外，須經授權始得於傳輸期間內閱讀、複製、修改或移除個人資料。

在透過實體方式輸送資料載體之處，應於 SAP 採取充足措施，以確保達到約定服務水準 (例如：加密以及襯鉛容器)。

- Personal Data transfer over SAP internal networks are protected in the same manner as any other confidential data according to SAP Security Policy.

  於 SAP 內部網路間傳輸之個人資料，應受與 SAP 安全政策之任何其他機密資料相同之保護。

- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

  該資料於 SAP 與其客戶間傳輸時，對於傳輸個人資料之保護措施應經合意並成為相關合約之一部分。本規定適用於實體與網路之資料傳輸。客戶應於任何情況下承擔於 SAP 控管系統外進行資料傳輸之風險 (例如：自 SAP 資料中心之 防火牆外部傳輸資料)。

1.5 Data Input Control.

資料輸入控制

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

應可回溯檢查並確定是否已從 SAP 資料處理系統輸入、修改或移除個人資料及執行前開作業之人員。

Measures:

措施：

- SAP only allows authorized persons to access Personal Data as required in the course of their work.

  SAP 僅允許授權人員在其工作過程中依需要存取個人資料。

- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within SAP's Products and Services to the fullest extent possible.

  SAP 建置一套記錄系統，儘可能最大限度地供 SAP 或其分包處理商於 SAP 產品與服務內輸入、修改與刪除或屏蔽個人資料。

1.6 Job Control.

作業控制

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer.

受託處理之個人資料 (亦即代表客戶處理之個人資料) 僅應依相關合約及客戶相關指示進行處理。

Measures:

措施：

- SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, subprocessors or other service providers.

  SAP 使用控制和處理程序確保符合 SAP 與其客戶、分包處理商或其他服務提供商之間的契約。

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

  作為 SAP 安全性政策之一部分，個人資料之保護程度至少應達 SAP 資訊分級標準規定之「機密」資訊等級。

- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

  所有 SAP 員工及訂約分包處理商或其他服務提供商皆受契約之約束，需遵循所有敏感資訊的保密性，包括有關 SAP 客戶及夥伴之商業機密。

- For on premise support services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge or full active participation of the customer.

  對於內部部署支援服務，SAP 提供特別指定的安全支援票設施，並在該設施中提供具備特殊存取控制和受監控的安全區域，以便傳輸存取資料和密碼。SAP 客戶可隨時控制其遠端支援連線。SAP 員工需知會客戶或使其積極參與，始得存取客戶系統。

1.7 Availability Control.

可用度控制

Personal Data will be protected against accidental or unauthorized destruction or loss.

個人資料應受保護以防意外或未經授權之損毀或丟失。

Measures:

措施：

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.

  SAP 採用備份處理程序和其他措施，確保必要時快速恢復關鍵業務系統。

- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.

  SAP 亦使用不斷電供應系統 (例如：UPS、電池、發電機等)，確保資料中心不斷電。

- SAP has defined contingency plans as well as business and disaster recovery strategies for the provided Services.

  SAP 已定義所供服務之緊急應變計畫 以及商業與災後復原策略。

- Emergency processes and systems are regularly tested.

  需定期測試緊急處理程序和系統。

1.8 Data Separation Control.

資料分離控制

Personal Data collected for different purposes can be processed separately.

出於不同目的收集之個人資料可以單獨處理。

Measures:

措施：

- SAP uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.

  SAP 使用部署軟體 (例如：多使用者或獨立系統架構) 之技術功能，達成多位客戶間個人資料之資料分離。

- Customers (including their Affiliates) have access only to their own data.

  客戶 (包括其關係企業) 僅可存取其本身的資料。

- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

若處理特定客戶的支援事件需要個人資料，則該資料乃係分配予特定訊息，並限用於處理該訊息，而非可供處理任何其他訊息存取之用。該資料係儲存在指定之支援系統。

1.9 Data Integrity Control .

資料完整性控制

Personal Data will remain intact, complete and current during processing activities.

個人資料於處理過程中將維持完好、完整與即時性。

Measures:

措施：

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

SAP 已建置多層防護措施，以防範未經授權之修改。

In particular, SAP uses the following to implement the control and measure sections described above. In particular:

SAP 特別使用下列項目來落實上述控制與措施條款之規範。特別是：

- Firewalls;
  防火牆；
- Security Monitoring Center;
  安全監視中心；
- Antivirus software;
  防毒軟體；
- Backup and recovery;
  備份與還原；
- External and internal penetration testing;
  外部與內部普及率測試；
- Regular external audits to prove security measures.
  檢驗安全措施之定期外部稽核。