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 and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

目的和適用性。本文件 (「**DPA**」) 已納入合約，並構成 SAP 與客戶間的書面 (包括電子形式) 合約之一部份。本 DPA 適用於 SAP 及其分包處理商在提供雲端服務時所處理的個人資料。若非正式運作環境是由 SAP 所提供，則本 DPA 不適用於雲端服務的此類環境，且客戶不得將個人資料儲存在此類環境中。

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

結構。附錄 1 和 2 已納入本 DPA 並構成本 DPA 之一部份。其中列出經合意的處理對象、處理性質和處理目的、個人資料類型、資料當事人類別，以及適用的技術和組織措施。

1.3 GDPR. SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

GDPR。SAP 和客戶同意，雙方有責任審查並採納《一般資料保護規則》2016/679 (以下簡稱「**GDPR**」) 針對控管者及處理者所實施的要求，特別是 GDPR 第 28 條和第 32 條至第 36 條中，適用於根據 DPA 之規定所處理的客戶/控管者個人資料之要求。本 DPA 於附錄 3 中列出相關的 GDPR 要求和對應章節，以作說明。

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

管理。根據 DPA，SAP 為處理者，而其允許使用雲端服務的客戶和其他實體，則為控管者。客戶為單一聯絡人，並全權負責根據本 DPA 取得個人資料處理的相關授權、同意和權限，其中包括控管者在適用情況下核准以 SAP 為處理者。在客戶提供授權、同意、指示或權限時，不僅代表客戶提供，而且代表使用雲端服務的其他控管者提供。若 SAP 通知客戶或向客戶發出通知，客戶允許控管者使用雲端服務則視為收到這些資訊或通知，而客戶有責任將此類資訊和通知轉發至相關控管者。

2. SECURITY OF PROCESSING
處理之安全性

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

適當技術和組織措施。SAP 已建置並將使用 附錄 2 所規定的技術和組織措施。客戶已審查這類措施，並同意對於客戶在訂購單中選擇的雲端服務，考慮到處理個人資料的最先進技術、建置成本、性質、範圍、內容和目的，這些措施是適當的做法。

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

變更。對於託管在同一資料中心，並接收相同的雲端服務的整個客戶群，SAP 將附錄 2 所規定的技術和組織措施應用於整個客戶群。在安全性等級維持不變或更佳的前提下，SAP 有權隨時更改附錄 2 所列出的措施，恕不另行通知。只要個別措施與新措施兩者可以獲致相同目的，且不會降低個人資料保護的安全等級，則個別措施可以由新措施所取代。

3. SAP OBLIGATIONS
SAP 義務

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

客戶指示。SAP 將僅根據經過記錄的客戶指示處理個人資料。合約 (包括本 DPA) 構成此類經過記錄的初步指示，並且每次使用雲端服務均構成進一步指示。SAP 將採取合理措施以遵守其他客戶指示，唯該指示須符合資料保護法之要求、技術上可行，且不須變更雲端服務。若發生前述例外情況，或 SAP 無法遵守指示，或認為該指示違反資料保護法，則 SAP 將立即通知客戶 (可透過電子郵件通知)。

3.2 Processing on Legal Requirement. SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

法規要求之處理。SAP 可能根據適用法律之規定來處理個人資料。在此情況下，SAP 應於處理之前告知客戶該法規要求，除非該法律基於重要的公共利益理由而禁止該項資訊。

3.3 Personnel. To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

人員。SAP 及其分包處理商僅得向承諾保密該等資料的授權人員授予存取權限，以處理個人資料。SAP 及其分包處理商應對可存取個人資料之人員，定期舉行相關之資料安全性與資料隱私措施培訓。

3.4 Cooperation. At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

合作。應客戶之請求，凡資料當事人或監管機關就 SAP 處理個人資料或任何個人資料之侵害提出要求，SAP 將合理配合客戶和控管者處理之。當 SAP 收到來自資料當事人的個人資料處理相關請求時，將在合理可行的前提下盡快通知客戶，且如可行的話，不會在沒有客戶進一步指示的情況下，自行回覆此類請求。SAP 應提供支援客戶從雲端服務修正或移除個人資料，或根據資料保護法限制處理個人資料之功能。若未提供此類功能，SAP 將根據客戶指示和資料保護法，修正或刪除個人資料，或限制處理個人資料。

3.5 Personal Data Breach Notification. SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

個人資料侵害通知。SAP 將在知悉個人資料侵害情形後不無故拖延的通知客戶，並提供所持有的合理資訊，以協助客戶履行依據資料保護法之要求回報個人資料侵害之義務。SAP 得按可獲得資訊的時機分階段提供之。此類通知不應理解或解釋為 SAP 承認過失或法律責任。

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

資料保護影響評估。若依據資料保護法規定，客戶 (或其控管者) 必須執行資料保護影響評估或事先諮商主管機關，SAP 將按客戶要求，提供一般可用於雲端服務的文件 (例如，本 DPA、合約、稽核報告或認證)。任何額外協助應由雙方協議。

4. DATA EXPORT AND DELETION
資料匯出與刪除

4.1 Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data.

客戶匯出和檢索。在訂閱期間內，客戶可以根據合約隨時存取其個人資料。客戶得以標準格式匯出和檢索其個人資料。匯出和檢索可能受限於技術，在此情況下，SAP 和客戶應找出客戶存取個人資料之合理方式。

4.2 Deletion. Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless

applicable law requires retention.

刪除。在訂閱期間屆滿之前，客戶得使用 SAP 自助匯出工具 (如適用)，自雲端服務執行個人資料最終匯出作業 (此將構成個人資料的之「返還」）。在訂閱期間結束時，客戶茲指示 SAP 依據資料保護法在合理期間內(不超過六個月)刪除託管雲端服務伺服器上之剩餘個人資料，除非適用法律要求保留。

5. CERTIFICATIONS AND AUDITS
認證及稽核

5.1 Customer Audit. Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

客戶稽核。客戶或 SAP 可合理接受的獨立第三方稽核員 (不包括 SAP 任何競爭對手，或不具適當資格或獨立性的第三方稽核員)，得稽核與 SAP 個人資料處理相關的控制環境和安全性措施，唯須符合下列條件：

(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 or other SOC1-3 attestation report. Upon Customer's request 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正式運作系統之技術及組織措施：(i) 符合 ISO 27001 或其他標準之認證 (範圍如認證所定義)；或 (ii) 有效之 ISAE3402 和/或 ISAE3000 或其他 SOC1-3 鑑定報告。於客戶要求時，可透過第三方稽核員或 SAP 提供稽核報告或 ISO 認證；

(b) A Personal Data Breach has occurred;
發生個人資料侵害：

(c) An audit is formally requested by Customer's data protection authority; or
稽核請求係由客戶的資料保護主管機關所正式提出；或

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.
資料保護法之強制規定提供客戶直接稽核之權利，並規定客戶僅得於十二個月內稽核一次，除非資料保護法之強制規定要求更頻繁的稽核次數。

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

其他控管者稽核。其他控管者得按第 5.1 條規定稽核 SAP 與個人資料處理相關的控制環境和安全性措施，唯須符合第 5.1 條所列適用於其他控管者之情況。此類稽核必須由客戶負責執行，如第 5.1 條中所述，除非資料保護法規定稽核必須由其他控管者執行。如稽核要求是由 SAP 根據合約處理其個人資料的多個控管者提出，則客戶應使用一切合理方式合併稽核次數，以避免重複稽核。

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit

reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

稽核範圍。客戶應於稽核前至少六十天發出通知，除非資料保護法強制規定或適格的資料保護主管機關要求較短的通知期限。各方當事人應以合理且誠信的方式，共同協議稽核頻率和範圍。客戶的稽核時間應以最多三個工作日為限。除上述限制之外，各方當事人將利用現有認證或其他稽核報告，以避免或盡可能減少重複稽核。客戶應向 SAP 提供一切稽核結果。

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

稽核費用。客戶應承擔所有稽核費用，除非此類稽核揭露 SAP 對本 DPA 有重大違反情事，則 SAP 應自行承擔稽核費用。若稽核判定 SAP 違反本 DPA 所規定之義務，SAP 應立即自費予以補正。

6. SUBPROCESSORS

分包處理商

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

許可的用途。SAP 具有將個人資料處理分包至分包處理商之一般授權，唯須符合下述情況：

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

SAP 或的 SAP SE，應以自己名義，並以書面形式 (包括電子形式) 與分包處理商訂立合約，合約應符合本 DPA 有關分包處理商處理個人資料之條款。SAP 應依據合約條款對分包處理商違反之行為負責；

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

SAP 將於選任分包處理商前評估其安全性、隱私性和機密性措施，以確保其可符合本 DPA 所要求的個人資料保護等級；以及

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

SAP 發佈在合約生效日已備妥之分包處理商清單，或根據客戶請求向其提供清單，其中包括 SAP 用於提供雲端服務的各分包處理商名稱、地址和角色。

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

新分包處理商。SAP 得自行決定對分包處理商之任用，唯須符合下列規定：

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

任何增加或替換分包處理商名單(包含新分包處理商的名稱、地址和角色)前，SAP 將(以電子郵件或透過 SAP Support 可公佈於 Support Portal)事先通知客戶；以及

(b) Customer may object to such changes as set out in Section 6.3.

客戶可依第 6.3 條所述，對此類變更表示反對。

6.3 Objections to New Subprocessors.
對新分包處理商之異議。

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

若客戶依據資料保護法中之合法理由反對由新分包處理商處理個人資料，則可以書面通知 SAP 終止合約(僅限於擬使用新分包處理商的雲端服務)。此項終止自客戶之指定時間起生效，最遲不應晚於 SAP 通知客戶新分包處理商之日起三十日。若客戶未於三十日內提出終止要求，則視為客戶接受新分包處理商。

(b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period.

在 SAP 通知客戶新分包處理商之日起三十日內，客戶得要求各方當事人就拒絕之意思秉持誠信一起商討解決方案。此項商討不得延長終止期限，且不會影響 SAP 於三十天後使用新分包處理商之權利。

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.
根據本 6.3 條規定發生之終止均不歸責於任何一方當事人，並應遵守合約之條款。

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.
緊急更換。若發生超出 SAP 合理控制範圍的原因，且基於安全性或其他緊急原因有緊急替換分包處理商之必要，則 SAP 得不經預告即替換分包處理商。在此情況下，SAP 應於委任替換的分包處理商後，盡快地將其資訊通知客戶。第 6.3 條適用此情況。

7. INTERNATIONAL PROCESSING
跨國處理

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

跨國處理之條件。在資料保護法許可範圍內，SAP 有權，包括使用分包處理商，於客戶所在國家以外地區依 DPA 處理個人資料。

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:
標準契約條款。若 (I) 位於 EEA 或瑞士的個人資料控管者，於 EEA、瑞士以外之國家，及於歐盟認可為安全國家以外的任何國家、組織或領土範圍內處理個人資料，並依 GDPR 第 45 條規範具備適當充分之資料保護等級,

或 (ii) 其他控管者之個人資料為跨國處理，控管者所在國家之法律要求採取適當措施進行此類跨國處理，且該等適當措施可透過簽訂標準契約條款達成，則：

(a) SAP and Customer enter into the Standard Contractual Clauses;
SAP 與客戶簽訂標準契約條款；

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or
客戶與各相關分包處理商簽訂之標準契約條款如下：(i) 客戶以權利與義務之獨立擁有人加入 SAP 或 SAP SE 與分包處理商所簽訂標準契約條款(即「參加模式」)，或 (ii) 分包處理商 (由 SAP 代表) 與客戶簽訂標準契約條款 (即「授權模式」)。若 SAP 已根據第 6.1(c) 條所提供的分包處理商清單或向客戶發出的通知，且明示確認分包處理商符合授權模式之條件，則適用授權模式；和/或

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.
其他已獲客戶依合約授權使用雲端服務之控管者，亦可按上述第 7.2 (a) 條和 (b) 條之相同方式，與 SAP 和/或相關分包處理商簽訂標準契約條款。在此情況下，客戶將代表其他控管者簽訂標準契約條款。

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.
標準契約條款與合約之關係。合約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。為免疑義，本 DPA 於第 5 條和第 6 條中進一步說明之稽核與分包處理商規則，同樣適用於標準契約條款。

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.
標準契約條款之適用法律。標準契約條款應受相關控管者註冊成立所在國家的法律管轄。

8. DOCUMENTATION; RECORDS OF PROCESSING
文件；處理記錄

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.
各方當事人均有責任遵守文件要求，特別是根據資料保護法之要求保存處理記錄。各方當事人應合理協助他方符合文件要求，包括以他方所要求的合理方式 (例如使用電子系統) 提供其所需資訊，以使他方得以遵守有關維護處理記錄之義務。

9. EU ACCESS
EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this

Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply.

選購服務。EU Access 為 SAP 所提供的選購服務。SAP 應根據本第 9 條，提供僅為正式運作執行個體適用 EU Access 的雲端服務。若雙方未於訂購單中明確規定且同意 EU Access，則本第 9 條並不適用。

9.2 **EU Access.** SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

EU Access。除非客戶以書面形式(允許使用電子郵件)明確依個案授權，或符合第 9.4 條中的例外情況，否則 SAP 僅會使用歐洲分包處理商提供需存取雲端服務個人資料的支援，SAP 亦不得將個人資料匯出 EEA 或瑞士境外。

9.3 **Data Center Location.** Upon the effective date of the Agreement, 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.

資料中心地點。自合約生效日起，用於託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。

9.4 **Exclusions.** The following Personal Data is not subject to 9.2 and 9.3:
例外狀況。以下的個人資料不受 9.2 和 9.3 之約束：

(a) Contact details of the sender of a support ticket; and
支援單傳送者的聯絡人詳細資料；以及

(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。

10. 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。

10.1 **"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; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.
「**控管者**」係指單獨或與他人共同決定處理個人資料之目的和手段的自然人或法人、政府機構、機關或其他法律主體；就本 DPA 而言，若客戶充當另一控管者的處理者，則 SAP 應將其視為額外且獨立的控管者，並具有本 DPA 規定的個別控管者之權利和義務。

10.2 **"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或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 。

10.3 **"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 (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

「**資料保護法**」係指根據合約處理個人資料時，用於保護當事人基本權利和自由及其隱私權的適用法律（針對 SAP 代表客戶處理個人資料之情況，相關當事人間之關係以 GDPR 為最低標準，不論個人資料是否適用 GDPR)。

10.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

「**資料當事人**」係指資料保護法所定義的已識別或足資識別之自然人。

10.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein 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。

10.6 **"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。

10.7 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) 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 (as defined under the Agreement).

「**個人資料**」係指受資料保護法保護的資料當事人相關資料。就 DPA 而言，上述資料僅包括下列個人資料：(i) 由客戶或其授權使用者輸入或由使用雲端服務衍生，或 (ii) 提供給 SAP 或其分包處理商或由其存取，以依據合約提供支援。個人資料為客戶資料的其中一部份 (如合約所定義)。

10.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

「**個人資料侵害**」係指已確認之 (1) 個人資料之意外或非法破壞、遺失、更改、未經授權之揭露或第三方未經授權之存取，或 (2) 涉及個人資料的類似事件，控管者必須根據資料保護法之規定，向各個案之適格資料保護主管機關或資料當事人提供通知。

10.9 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

「**處理者**」係指代表控管者處理個人資料的自然人或法人、政府機構、機關或其他法律實體，直接作為控管者的處理者或間接作為處理者的分包處理商，代表控管者處理個人資料。

10.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.

「**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)) 或任何歐盟委員會發行之後續版本 (其應自動適用)。在本合約生效日當時所適用的標準契約條款附於附錄 4。

10.11 "Subprocessor" means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

「分包處理商」係指 SAP 關係企業、SAP SE、SAP SE 關係企業，以及 SAP、SAP SE 或 SAP SE 關係企業所委任的第三方，用於根據本 DPA 處理與雲端服務相關的個人資料。

11. GOVERNING LANGUAGE

準據語言

This DPA is executed in both Chinese and English languages. In the event that there are different interpretations of the same provision or actual contradictions between the two languages, the meanings of the English version shall prevail.

本 DPA 以中文及英文簽署。如中英文版中就相同條款之解釋有所歧義或兩者互相抵觸時，應以英文版為準。

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 附錄 1 及標準契約條款(若有適用)

Data Exporter
資料匯出者
The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.
資料匯出者為訂閱雲端服務之客戶，該服務允許授權使用者輸入、修訂、使用、刪除或以其他方式處理個人資料。若客戶允許其他控管者使用雲端服務，則該控管者亦為資料匯出者。

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 SE 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 SE 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 SE 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 SE 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
資料當事人
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當事人：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 Agreement (including the Order Form) if any.
傳輸之個人資料涉及下列特殊的資料類別：如合約 (包括訂購單) 中所規範 (如有)。

Processing Operations / Purposes
處理作業/目的
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 the Agreement.
  依據本合約履行客戶指示。

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures
DPA 附錄 2 及標準契約條款 (若有適用) - 技術和組織措施

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):
本附錄 2 包括兩組技術和組織措施（"**技術和組織措施**"）：

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.
  第一組技術和組織措施（最近一次更新在 2018 年 4 月，未有變更）：適用於所有雲端服務，以下所定義的第二組技術和組織措施服務除外。

- **TOMs Set 2:** applies to the TOMs Set 2 Services only. As of May 4, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud, SAP SuccessFactors and SAP Cloud Platform. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.
  第二組技術和組織措施：只適用於第二組技術和組織措施服務。截至 2020 年 5 月 4 日，"**第二組技術和組織措施服務**" 係指下列雲端服務：SAP Analytics Cloud、SAP SuccessFactors 及 SAP Cloud Platform。SAP 可不時從第二組技術和組織措施服務列表中移除一項雲端服務。在此情況下，該雲端服務將受第一組技術和組織措施之約束。

TOMs SET 1
第一組技術和組織措施

Last Updated: April 2018
最近一次更新：2018 年 4 月

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

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
下列條款係定義 SAP 目前的技術和組織措施。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。只要個別措施與新措施兩者可以獲致相同目的，且不會降低個人資料保護的安全等級，則個別措施可以由新措施所取代。

1.1 Physical Access Control. 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.
實體存取控制。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 the SAP Security Policy
  SAP 使用以 SAP 安全政策為基礎的適當方式保護其資產和設施。
- 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 所有地點必須配戴識別證。

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 protect 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。為保護適當之功能，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 authorized personnel 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 私領域之授權人員姓名與進入時間。

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.
系統存取控制。應防止提供雲端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. Authorizations are managed via defined processes according to the SAP Security Policy
  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。授權是根據 SAP 安全政策並透過定義的程序管理。
- All personnel access SAP's systems with a unique identifier (user ID).
  所有人員皆使用唯一識別碼 (使用者 ID) 存取 SAP 系統。
- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their 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 SAP 安全政策 (例如，需授權才能授予權利) 得以實作。人員離職時，其存取權限將被撤銷。
- 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。分配用於驗證之個人化使用者 ID。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 provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.
  採用安全性補綴程式管理以確提供相關安全性更新之常態與定期部署。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. 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.
資料存取控制。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 Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
  在「有知情需要」的基礎上授予個人資料的存取權限。各人員可以存取用於履行職責的必要資訊。SAP 所使用的授權概念會記錄授予程序，及每個帳戶指派的角色 (使用者 ID)。所有客戶資料均按照 SAP 安全政策加以保護。
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data 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。保護處理個人資料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 software that has not been approved by SAP.
  SAP 不允許安裝未獲 SAP 核准之軟體。
- 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. Except as necessary for the provision of the Cloud Services in accordance with the 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 provide the agreed-upon service levels (for example, encryption and lead-lined containers).

資料傳輸控制。除了根據合約的雲端服務條款所必須者外，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承載媒介之處，應於 SAP 採取充足措施，以提供達到約定服務水準 (例如：加密以及襯鉛容器)。

Measures:

措施：

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  透過 SAP 內部網路傳輸之個人資料，應依照 SAP 安全政策保護。
- 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. 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.

資料輸入控制。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 personnel to access Personal Data as required in the course of their duty.
  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 the Cloud Service to the extent technically possible.
  SAP 已建置一套記錄系統，儘可能在技術可行的情況下，供 SAP 或其分包處理商於雲端服務內輸入、修改與刪除或凍結個人資料。

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

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

Measures:

措施：

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 使用控制和處理程序以監控是否符合 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，須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。

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

可用度控制。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 regular backup processes to provide restoration of business-critical systems as and when necessary.

  SAP 採用定期備份程序，以在必要時恢復重要企業系統之運作。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect 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 business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.

  SAP 為重要企業流程定義了企業應急計劃，並可為重要企業服務提供災難復原策略，其詳細資訊如相關雲端服務文件所述，或納入在雲端服務訂購單中。
- Emergency processes and systems are regularly tested.

  須定期測試緊急處理程序和系統。

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

資料分離控制。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。
- Customer (including its Controllers) has access only to its own data.

  客戶 (包括其控管者) 僅可存取其個人資料。
- If Personal Data is required to handle a support incident from 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. Personal Data will remain intact, complete and current during processing activities.

資料完整性控制。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。

TOMs SET 2
第二組技術和組織措施

(applies to TOMs Set 2 Services defined above)
適用於以上所定義的第二組技術和組織措施服務

Last Updated: May 4, 2020
最近一次更新：2020 年 5 月 4 日

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

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
下列條款係定義 SAP 目前的技術和組織措施。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。只要個別措施與新措施兩者可以獲致相同目的，且不會降低個人資料保護的安全等級，則個別措施可以由新措施所取代。

1.1 Physical Access Control.
實體存取控制。

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
  SAP 使用以 SAP 安全政策為基礎的適當方式保護其資產和設施。
- 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 所有地點必須配戴識別證。

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 protect 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。為保護適當之功能，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 authorized personnel 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 私領域之授權人員姓名與進入時間。

1.2 System Access Control.

系統存取控制。

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy.

  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。授權是根據 SAP 安全政策並透過定義的程序管理。
- All personnel access SAP's systems with a unique identifier (user ID).

  所有人員皆使用唯一識別碼 (使用者 ID) 存取 SAP 系統。
- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked.

  SAP 已有政策，旨在規定沒有權利會在未授權的情況下授予，而人員離職時，其存取權限將被撤銷。
- 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。分配用於驗證之個人化使用者 ID。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 processes to deploy relevant security updates on a regular and periodic basis.

  安全性補綴程式管理程序以定期進行相關安全性更新部署。
- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication.

  全部 SAP 公司之網路及重要設施之遠端途徑經經驗證受到保護。

1.3 Data Access Control.

資料存取控制。

- 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 Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.

  在「有知情需要」的基礎上授予個人資料的存取權限。各人員可以存取用於履行職責的必要資訊。SAP 所使用的授權概念會記錄授予程序，及每個帳戶指派的角色 (使用者 ID)。所有客戶資料均按照 SAP 安全政策加以保護。

- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and/or 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。保護處理個人資料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/或滲透測試。
- Processes and policies to detect the installation of unapproved software on production systems.
  偵測在正式運作系統安裝未獲核准之軟體的程序與政策。
- 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。

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  透過 SAP 內部網路傳輸之個人資料，應依照 SAP 安全政策保護。
- 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。

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
  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 in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.
  SAP 已在大多情況建置一套記錄系統，儘可能在技術可行的情況下，供 SAP 或其分包處理商於雲端服務內輸入、修改與刪除或凍結個人資料。

1.6 Job Control.
工作控制。

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 使用控制和處理程序以監控是否符合 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，須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。

1.7 Availability Control.

可用度控制。

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
  SAP 採用定期備份程序，以在必要時恢復重要企業系統之運作。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect 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 business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
  SAP 為重要企業流程定義了企業應急計劃，並可為重要企業服務提供災難復原策略，其詳細資訊如相關雲端服務文件所述，或納入在雲端服務訂購單中。
- Emergency processes and systems are regularly tested.
  須定期測試緊急處理程序和系統。

1.8 Data Separation Control.

資料分離控制。

- 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。
- Customer (including its Controllers) has access only to its own data.
  客戶 (包括其控管者) 僅可存取其個人資料。
- If Personal Data is required to handle a support incident from 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。

- 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.
  SAP 特別使用下列項目來落實上述控制與措施條款之規範。
- 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 and/or regular external audits to prove security measures.
  外部與內部普及率測試和/或檢驗安全措施之定期外部稽核。

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 附錄 3 及適用之標準契約條款

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

下表列出 GDPR 相關條款和 DPA 的對應條款，僅供說明之用。

Article of GDPR **GDPR 之條款**	**Section of DPA** **DPA 之條款**	**Click on link to see Section** **按一下連結以查看條款**
28(1) 第 28(1) 條	2 and Appendix 2 2 和附錄 2	Security of Processing and Appendix 2, Technical and Organizational Measures. Security of Processing 以及附錄 2，技術和組織措施。
28(2), 28(3) (d) and 28 (4) 第 28(2)、28(3) (d) 和 28 (4) 條	6	SUBPROCESSORS SUBPROCESSORS
28 (3) sentence 1 第 28 (3) 條第 1 句	1.1 and Appendix 1, 1.2 1.1 和附錄 1、1.2	Purpose and Application. Structure. Purpose **and Application.**。Structure**.**。
28(3) (a) and 29 第 28(3) (a) 和 29 條	3.1 and 3.2 3.1 和 3.2	Instructions from Customer. Processing on Legal Requirement. Instructions **from Customer.** Processing **on Legal Requirement.**
28(3) (b) 第 28(3) (b) 條	3.3	Personnel. Personnel
28(3) (c) and 32 第 28(3) (c) 和 32 條	2 and Appendix 2 2 和附錄 2	Security of Processing and Appendix 2, Technical and Organizational Measures. Security of Processing 以及附錄 2，技術和組織措施。
28(3) (e) 第 28(3) (e) 條	3.4	Cooperation. Cooperation**.**
28(3) (f) and 32-36 第 28(3) (f) 和 32-36 條	2 and Appendix 2, 3.5, 3.6 2 和附錄 2、3.5、3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment. Security of Processing 以及附錄 2，技術和組織措施。 Personal **Data Breach Notification.** Data Protection Impact Assessment.
28(3) (g) 第 28(3) (g) 條	4	Data export and Deletion Data export and Deletion
28(3) (h) 第 28(3) (h) 條	5	CERTIFICATIONS AND AUDITS CERTIFICATIONS AND AUDITS
28 (4) 第 28 (4) 條	6	SUBPROCESSORS SUBPROCESSORS
30 第 30 條	8	Documentation; Records of processing Documentation; Records of processing
46(2) (c) 第 46(2) (c) 條	7.2	Standard Contractual Clauses Standard Contractual Clauses.

Appendix 4
附錄 4

The Standard Contractual Clauses set out in this Appendix 4 are current as at 31 March 2018, and the Chinese translation is provided as a matter of convenience only. The English language version controls. These Standard Contractual Clauses are automatically subject to updates by the European Commission and as subsequently published by the European Commission, Customer should always access the URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 for updated versions of the Standard Contractual Clauses. Customer's local language may not be supported at the European Commission, or at its URL, and it will be Customer's responsibility to ensure that it is aware of the current version/s of the Standard Contractual Clauses and to manage for itself and its Controllers all required translations of any updated Standard Contractual Clauses. // 本附錄 4 所載的標準契約條款為於 2018 年 3 月 31 日之最新版本，而中譯文僅為方便起見而提供，以英文版為準。這些標準契約條款自動受歐盟委員會的更新並隨後由歐盟委員會發布，對於標準契約條款的更新版本，客戶應自行查閱下列連結 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri =celex%3A32010D0087。歐盟委員會或上述連結可能不會有客戶的本地語言版本，客戶有責任確保其了解當前版本的標準契約條款，並為其自身及其控管者管理任何更新之標準契約條款的必要翻譯。

STANDARD CONTRACTUAL CLAUSES (PROCESSORS) // 標準契約條款 (處理商)[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection
為達歐盟指令 95/46/EC 第 26(2) 款 (或自 2018 年 5 月 25 日起實施之法規 2016/79 之第 44 條及其後續條文）之目的，對於將個人資料傳輸到第三方國家中但無法確保提供足夠資料保護層級的處理商

Customer also on behalf of the other Controllers // **客戶同時代表其他控管者**
(in the Clauses hereinafter referred to as the '**data exporter'**) // (以下簡稱「**資料匯出者**」)
and // 與
SAP
(in the Clauses hereinafter referred to as the **'data importer'**) // (以下簡稱「**資料匯入者**」)

each a 'party'; together 'the parties' // 分別稱「當事人」；統稱「雙方」，

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1. // 雙方業已就下列契約條款 (以下稱「條款」) 達成合意，當資料匯出者傳輸附錄 1 所定之個人資料予資料匯入者時，得就保護個人隱私、基本權利和個人之自由提供足夠的保障。

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU) // 根據 2010 年 2 月 5 日歐盟委員會決議 (2010/87/EU)

Clause 1 // 第 1 條

Definitions // 名詞定義

For the purposes of the Clauses:
對本條款而言：

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
本條款所指「個人資料」、「特殊的資料類別」、「流程/處理」、「控管者」、「處理商」、「資料當事人」與「監管機關」，意義應同於歐洲議會和歐洲理事會於 1995 年 10 月 24 日就個人保護議題中有關個人資料處理和自由移動發佈之指令 95/46/EC 所載。

(b) 'the data exporter' means the controller who transfers the personal data;
「資料匯出者」係指傳輸個人資料之控管者；

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
「資料匯入者」係指同意自資料匯出者處接收個人資料之處理者，該處理者乃是為在傳輸後依據資料匯出者之指示與條款之規定，而代表資料匯出者執行處理作業，同時不受第三國系統之約束，以確保在指令 95/46/EC 第 25(1) 條含意內提供適當之保護；

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
「分包處理商」係指資料匯入者所雇用，或資料匯入者之其他任何分包處理商所雇用（該資料匯入者同意自資料匯入者處或自資料匯入者之任何其他分包處理商處，接收個人資料）之處理者，該處理者乃是專為在傳輸後依據資料匯入者之指示、條款之規定以及書面轉包條款之規定，而代表資料匯出者執行處理作業；

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
「適用資料保護法」係指保護個人基本權利和自由的法律，這些權利中尤其關於處理個人資料的隱私權，適用於確定資料匯出者所在歐盟/歐洲經濟區成員國中的資料控管者；

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
「技術和組織安全措施」係指旨在保護個人資料的措施，使其免受意外或非法損毀或意外丟失、篡改、未經授權揭露或存取、尤其是處理工作涉及到透過網路傳輸以及針對所有其他非法形式的處理時。

Clause 2 // 第 2 條

Details of the transfer // 傳輸詳細資料

The details of the transfer and in particular the special categories of personl data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
傳輸詳細資料 (若適用，尤其是特殊類別的個人資料) 於附錄 1 中明定，該附錄構成本條款不可或缺的一部分。

Clause 3 // 第 3 條

Third-party beneficiary clause // 第三方受益人條款

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
作為第三方受益人條款，資料當事人得對資料匯出者強制執行本條、第 4(b) 條至 (i) 條、第 5(a) 條至 (e) 條、(g) 條至 (j) 條、第 6(1) 條和 (2)條、第 7 條、第 8(2) 條與第 9 條至第 12 條之規定。

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
資料當事人得對資料匯入者強制執行本條、第 5(a) 條至 (e) 條、(g) 條、第 6 條、第 7 條、第 8(2) 條與第 9 條至第 12 條之規定，緣由是資料匯出者實際上已消失或在法律上不再存在，除非任何繼受實體已承擔資料匯出者依合約或法律規定需承擔的全部法律義務而承擔資料匯出者的權利和義務，在此情況下，資料當事人始得對是類實體強制執行該等義務。

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
資料當事人得對分包處理商強制執行本條、第 5(a) 條至 (e) 條、(g) 條、第 6 條、第 7 條、第 8(2) 條與第 9 條至第 12 條之規定，緣由是資料匯出者和資料匯入者實際上均已消失或在法律上不再存在或變得無力償債，除非任何繼受實體已承擔資料匯出者依合約或法律規定需承擔的全部法律義務而承擔資料匯出者的權利和義務，在此情況下，資料當事人始得對是類實體強制執行該等義務。分包處理商的此第三方責任限於條款下其自身的處理作業。

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.
若資料當事人明確表達此願望並且國家法律允許，雙方不反對資料當事人由協會或其他機構代表。

Clause 4 // 第 4 條

Obligations of the data exporter // 資料匯出者之義務

The data exporter agrees and warrants:
資料匯出者同意並保證：

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
已根據適用的資料保護法之相關條款處理並將繼續處理（包括傳輸本身）個人資料（並且，若有適用，已通知資料匯出者所在成員國的相關機構）並且不違反此成員國的相關條款；

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
已指示、並在個人資料處理服務期間將指示資料匯入者，僅以資料匯出者的名義，並根據適用的資料保護法及本條款之規定，處理所傳輸的個人資料；

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
資料匯入者將就本合約附錄 2 中明定之技術和組織安全措施提供足夠的保證；

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
在評估適用的資料保護法要求後，安全措施可以適當保護個人資料，使其免於遭受意外或非法損毀或意外喪失、篡改、未經授權揭露或存取，特別是處理涉及到透過網路傳輸資料時，以及針對所有其他非法形式的處理，並且這些措施可確保處理所產生之風險和最新技術水準和執行之成本達到一定的安全層級；

(e) that it will ensure compliance with the security measures;
將保證遵守安全措施；

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
(f) 若傳輸涉及特殊類別的資料，則資料當事人已獲通知並將在資料可傳輸到未在指令 95/46/EC 含意內提供充足保護之第三國家之前或之後盡快獲得通知；

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

若資料匯出者決定繼續傳輸或取消暫停，則將根據第 5(b) 條和第 8(3) 條，轉寄從資料匯入者或任何分包處理商接收的任何通知給資料保護監管機關；

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

一經請求，向資料當事人提供本條款之副本 (附錄 2 除外)、安全措施的概括性描述，以及須依本條款訂定分包處理服務合約之副本，除非本條款或合約包括商業資訊，在此情況下，資料匯入者得移除該商業資訊；

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

分處理之處理作業，將由分包處理商根據第 11 條執行，其所提供之個人資料與資料當事人權利保護層級，應同於本條款下之資料匯入者；以及

(j) that it will ensure compliance with Clause 4(a) to (i).

將確保符合第 4(a) 至 (i) 條。

Clause 5 // 第 5 條

Obligations of the data importer // 資料匯入者之義務

The data importer agrees and warrants:
資料匯入者同意並保證：

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

僅以資料匯出者名義處理個人資料，並應遵照資料匯出者之指示和本條款之規定；倘由於任何因素無法遵照前開指示或規定，分包處理商同意將無法遵循之情事，盡速知會資料匯出者，而在該情況下，資料匯出者有權停止資料傳輸，及/或終止本合約；

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

並無理由足信存在任何適用之法律，可妨礙其履行從資料匯出者收到的指示和其在本合約下的義務，倘若該法律有所變更，可能對本條款所設之保證和義務產生重大不利影響，則其在知悉時，便將盡速通知資料匯出者該變更，而在此情況下，資料匯出者有權暫停傳輸資料，及/或終止本合約；

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

在處理所傳輸的個人資料前，業已執行附錄 2 中所定之技術和組織安全措施；

(d) that it will promptly notify the data exporter about:
其會盡速將下列情事，知會資料匯出者：

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
執法機關對於揭露個人資料之任何具法律拘束力之要求，除非另行禁止，例如刑法為了保護執法調查之機密性所為之禁止規定；

(ii) any accidental or unauthorised access; and
任何意外或未經授權的存取；以及

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
直接從資料當事人接收的任何請求，而不回應該請求，除非另行取得這樣做的授權；

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
盡速正確處理來自資料匯出者關於處理待傳輸之個人資料的所有詢問，受傳輸約束並遵守監管機關關於處理所傳輸資料的建議；

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
根據資料匯出者的請求，提供資料處理設施，以備對於本條款所涵蓋的處理作業，進行稽核；前開稽核，應由資料匯出者或由獨立成員組成、並具有必要的專業資格、且負有保密義務而由資料匯出者選定 (如果適用，並應取得監管機關之同意) 之檢查機構執行；

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
一經請求，應向資料當事人提供本條款之副本或分處理之任何現有合約，除非本條款或合約含有商業資訊，而在該情況下，其得移除該商業資訊 (但附錄 2 除外，倘資料當事人無法從資料匯出者取得副本，附錄 2 應由安全措施的概括性描述替代)；

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
先前業已就分處理通知資料匯出者，並事先取得其書面同意；

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
處理服務將由分包處理商根據第 11 條之規定加以執行；

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

立即傳送一份根據條款訂立的次處理商合約副本給資料匯出者。

Clause 6 // 第 6 條

Liability // 責任

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

雙方同意，任何資料當事人由於任一方或分包處理商違反第 3 條或第 11 條之義務而遭受之損害，得向資料匯出者就該損害獲取賠償。

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

若資料當事人無法根據第 1 項之規定，針對資料匯入者或其分包處理商違反第 3 條或第 11 條之任何義務，對資料匯出者提出索賠，緣由是資料匯出者實際上已消失或在法律上不再存在或變得無力償債，則資料匯入者同意，資料當事人可將資料匯入者視為資料匯出者而提出索賠，除非任何繼受實體已承擔資料匯出者依合約或法律規定需承擔的全部法律義務，在此情況下，資料當事人始得對是類實體強制執行其權利。

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

資料匯入者不得依賴分包處理商違反其義務來避免其自身的責任。

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

若資料當事人無法根據第 1 項和第 2 項之規定，針對分包處理商違反第 3 條或第 11 條之任何義務，對資料匯出者或資料匯入者提出索賠，緣由是資料匯出者和資料匯入者實際上均已消失或在法律上不再存在或變得無力償債，則分包處理商同意，資料當事人可就本條款下資料分包處理商自身之處理作業，將分包處理商視為資料匯出者或資料匯入者而提出索賠，除非任何繼受實體已承擔資料匯出者或資料匯入者依合約或法律規定需承擔的全部法律義務，在此情況下，資料當事人始得對是類實體強制執行其權利。分包處理商的責任限於條款下其自身的處理作業。

Clause 7 // 第 7 條

Mediation and jurisdiction // 調解及管轄權

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

資料匯入者同意，若資料當事人行使第三方受益人權益和/或根據本條款對損害提出索賠，則資料匯入者會接受資料當事人的下列決定：

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

將爭議交由獨立人士 (或者，若有適用，交由監管機關) 進行調解；

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

將爭議提交給資料匯出者所在成員國中的法庭。

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

雙方同意，資料當事人進行的選擇不會損害根據國家或國際法律的其他條款尋求補救的實質性或程序權利。

Clause 8 // 第 8 條

Cooperation with supervisory authorities // 與監管機關合作

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

若監管機關作此要求或根據適用的資料保護法之規定應予提存時，資料匯出者同意提存一份本合約副本給監管機關。

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

雙方同意，監管機關有權對資料匯入者與任何分包處理商執行稽核，而該稽核所執行之範圍及應遵守之條件，應與根據適用的資料保護法對資料匯出者進行稽核時相同。

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

若存在可適用於資料匯入者或任何分理商而得妨礙對渠等進行第 2 項所述稽核之法律，資料匯入者應盡速將該情事知會資料匯出者。在此情況下，資料匯出者應有權採取第 5(b) 款中可預見的措施。

Clause 9 // 第 9 條

Governing law // 準據法

The Clauses shall be governed by the law of the Member State in which the data exporter is established.
本條款應以資料匯出者所在成員國的法律為準據法。

Clause 10 // 第 10 條

Variation of the contract // 合約變更

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.
雙方承諾不變更或修改本條款。這不排除雙方根據需要新增業務相關事宜的條款，惟該等條款不得與本條款牴觸。

Clause 11 // 第 11 條

Sub-processing // 分處理

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

除非事先取得資料匯出者之書面同意，否則資料匯入者不得分包其以資料匯出者名義依本條款規定所執行之任何處理作業。資料匯入者若需取得資料匯出者同意以分包其受本條款規範之義務，唯一的方式係向依本條款對分包處理商與資料匯入者課予相同義務之分包處理商，取得書面同意。在分包處理商無法根據此書面合約履行其資料保護義務時，資料匯入者應對根據此合約履行此次處理商義務對資料匯出者負全責。

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

資料匯入者與分包處理商事先訂定之書面合約並應就資料當事人無法依據第 6 條第 1 項規定，對資料匯出者或資料匯入者提出索賠之情況，如第 3 條之規定提供第三方受益人條款，緣由是資料匯出者和資料匯入者實際上均已消失或在法律上不再存在或變得無力償債，同時亦無繼受實體已承擔資料匯出者或資料匯入者依合約或法律規定需承擔的全部法律義務。分包處理商的此第三方責任限於條款下其自身的處理作業。

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

對於與第 1 段所載合約之分處理與資料保護方面的相關條款，應受確定資料匯出者所在成員國中的法律規範。

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

對於每年須更新一次以上的分處理合約，資料匯出者應保留一份清單，列出依本條款結束並由資料匯入者依第 5(j) 條規定提出通知者。該清單應可供資料匯出者之資料保護監管機關使用。

Clause 12 // 第 12 條

Obligation after the termination of personal data-processing services
終止個人資料處理服務後的義務

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

雙方同意，在終止提供資料處理服務後，資料匯入者和分包處理商應根據資料匯出者之選擇將所傳輸的所有個人資料及其副本返還予資料匯出者，或銷毀所有個人資料並向資料匯出者證明已完成該作為，除非法律強制禁止資料匯入者，將其所傳輸的個人資料之全部或一部，予以返還或銷毀。在此情況下，資料匯入者保證會確保所傳輸之個人資料的機密性並不再主動處理所傳輸的個人資料。

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

資料匯入者和分包處理商保證一經資料匯出者及/或監管機關之要求，便會提交其資料處理設施，以便進行第 1 項中所載之稽核措施。