PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES
SAP 云服务的个人数据处理协议

1. BACKGROUND
背景信息

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.

目的和应用。本文档（以下简称"**DPA**"）纳入协议并构成 SAP 与客户之间签订的书面（包括电子形式）合同的一部分。本 DPA 适用于 SAP 及其分处理方处理的与云服务的提供有关的个人数据。本 DPA 不适用于云服务的非生产环境，若 SAP 提供此类环境，客户不得在此类环境中存储个人数据。

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.

结构。附录 1 和 2 纳入本 DPA 并构成本 DPA 的一部分。这两个附录规定了约定的主旨，处理性质和目的，个人数据类型，数据当事人类别以及适用技术措施和组织措施。

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 和客户同意，各方有责任了解和遵循《通用数据保护条例》2016 年第 679 号（以下简称"**GDPR**"），尤其是 GDPR 第 28 条和第 32 至 36 条，对控制方和处理方的要求，但前提是适用于依据 DPA 处理的客户/控制方的个人数据。为便于说明，附录 3 列出了相关 GDPR 要求和本 DPA 中的对应小节。

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。SAP 作为处理方，客户和 SAP 允许其使用云服务的实体作为受 DPA 约束的控制方。客户作为单一联络点，全权负责获取依据本 DPA 处理个人数据所需的任何相关授权、同意和许可，包括控制方将 SAP 用作处理方的相应批准。一旦客户提供授权、同意、指示或许可，这些授权、同意、指示或许可不仅代表客户提供，还代表使用云服务的任何其他控制方提供。若 SAP 向客户发出信息或通知，此类信息或通知应视为由客户允许使用云服务的控制方所接收，客户应负责将此类信息和通知转发给相关控制方。

2. SECURITY OF PROCESSING
处理安全

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.

相应技术措施和组织措施。SAP 已实施并将采用附录 2 中规定的技术措施和组织措施。客户已查看此类措施并同意，关于客户在订购单中选择的云服务，采取的相应措施考虑目前的技术发展水平、实施成本，以及个人数据的处理性质、范围、背景和目的。

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.

变更。SAP 对在同一数据中心托管且接收相同云服务的整个 SAP 客户群应用附录 2 中规定的技术措施和组织措施。SAP 可随时变更附录 2 中规定的措施，且不需要另行通知，但前提是维持相当或更高的安全等级。各项措施可由具有相同作用的新措施替代，但不得降低个人数据保护的安全等级。

3. SAP OBLIGATIONS

SAP 的义务

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).

客户的指令。SAP 仅根据客户的书面指令处理个人数据。协议（包括本 DPA）构成此类初始书面指令，之后每次对云服务的使用构成进一步指令。SAP 将尽合理努力遵循任何其他客户指令，但前提是，这些指令必须符合数据保护法要求并在技术上可行，而且不要求对云服务进行任何更改。如果出现任何上述例外情况，或 SAP 无法遵从某项指令或认为某项指令违反了数据保护法，SAP 将立即通知客户（允许使用电子邮件的方式）。

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.

根据法律要求进行处理。如果适用法律要求，SAP 也可处理个人数据。在此类情况下，SAP 应在处理之前告知客户此类法律要求，除非该法律基于公共利益的重要依据禁止告知。

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.

人员。为处理个人数据，SAP 及其分处理方应仅向承诺保密的授权人员授予访问权限。SAP 及其分处理方应定期对获得个人数据访问权限的人员进行相应数据安全和数据隐私措施方面的培训。

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。如客户请求，SAP 应合理配合客户和控制方，协助其处理数据当事人或监管部门就 SAP 对个人数据的处理或任何个人数据违规提出的要求。SAP 应尽快将从数据当事人处收到的与个人数据处理有关的任何请求告知客户，若适用，在未得到客户进一步指令的情况下，无需自行回复此类请求。SAP 应提供相关功能，支持客户根据数据保护法的规定，更正或从云服务中删除个人数据，或限制数据的处理。若未提供此类功能，SAP 应根据客户的指令和数据保护法的规定，更正或删除任何个人数据，或限制数据的处理。

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.
个人数据违规通知。在发现任何个人数据违规行为后，SAP 应及时通知客户，并提供掌握的合理信息，协助客户履行根据数据保护法要求报告个人数据违规行为的义务。SAP 可分阶段提供此类可用信息。此类通知不得被误解为或理解为 SAP 对过错或责任的承认。

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.
数据保护影响评估。根据数据保护法，若客户（或其控制方）需要执行数据保护影响评估或需事先咨询监管机构，应客户请求，SAP 应提供针对云服务全面披露的此类文档（例如，本 DPA、协议、审计报告或认证）。任何其他协助须经双方共同约定。

4. DATA EXPORT AND DELETION
数据导出及删除。

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.
客户导出和检索。在租用期限内，按照协议规定，客户能够随时访问其个人数据。客户可以标准格式导出和检索其个人数据。导出和检索可能会受技术限制，在此情形下，SAP 与客户应共同找到一种合理的方法以使客户能够访问个人数据。

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.
删除。在租用期限届满之前，客户可以使用 SAP 的自助服务导出工具（视提供情况而定）执行个人数据从云服务中的最终导出操作（该操作应视为个人数据的“返还”）。在租用期限结束时，客户特此指示 SAP 在合理期限内（不得超过 6（六）个月），根据数据保护法规定删除托管云服务的服务器上保留的个人数据，除非适用法律要求保留这些数据。

5. CERTIFICATIONS AND AUDITS
认证和审计

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:

客户审计。客户或 SAP 合理认可的独立第三方审计机构（不包括属于 SAP 竞争对手或没有适当资格或非独立的任何第三方审计机构）可就 SAP 处理个人数据的 SAP 控制环境和安全实践进行审计，但前提是：

(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 未能提供以下任一证明，就保护云服务生产系统的技术措施和组织措施提供充分的合规证据：(i) 符合 ISO 27001 标准或其他标准（具体范围见证书中的定义）的证书；或 (ii) 有效的 ISAE3402 和/或 ISAE3000 或其他 SOC1-3 认证报告。一旦客户请求，审计报告或 ISO 证书应通过第三方审计机构或 SAP 提供；

(b) A Personal Data Breach has occurred;
出现个人数据违规行为；

(c) An audit is formally requested by Customer's data protection authority; or
客户的数据保护机构正式要求实施审计；或者

(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.
强制性数据保护法为客户提供直接审计权利，但前提是客户在任意十二（12）个月期限内仅执行一次审计，除非强制性数据保护法要求提高审计频率。

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.
其他控制方审计。任何其他控制方均可按照第 5.1 节的规定，就 SAP 处理个人数据的 SAP 控制环境和安全实践进行审计，但前提是，第 5.1 节所述的情况适用于此类其他控制方。根据第 5.1 节的规定，此类审计必须由客户执行，除非数据保护法要求必须由其他控制方自己执行。如果多个由 SAP 依据协议处理其个人数据的控制方要求审计，客户应采取一切合理措施整合这些审计，避免进行多次审计。

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.
审计范围。对于任何审计，客户应至少提前六十（60）天发出通知，除非强制性数据保护法或主管数据保护机构要求在较短的时间内发送通知。任何审计的频率和范围均须经双方共同合理、诚意约定。客户审计时间最多为三（3）个工作日。若超过此时间限制，双方应利用现有的证书或其他审计报告避免或最大限度减少重复审计工作。客户应向 SAP 提供任何审计的结果。

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.
审计费用。客户应承担任何审计费用，除非此类审计发现 SAP 实质性违反本 DPA，这种情况下，SAP 应自行承担审计费用。如审计发现 SAP 违反其在本 DPA 下的义务，SAP 应自担费用立即对违规行为进行补救。

6. SUBPROCESSORS
分处理方

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:
许可使用。SAP 获得将个人数据处理工作分包给分处理方的一般授权，但前提是：

(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 或代表 SAP 的 SAP SE 就分处理方对个人数据的处理，通过与本 DPA 条款一致的书面合同（包括电子形式）聘用分处理方。根据本协议条款，SAP 应对分处理方的任何违约行为承担责任；

(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
在选择分处理方之前，SAP 应评估分处理方在安全、隐私和保密方面的实践，确定其有能力提供本 DPA 中要求的个人数据保护等级；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 将发布在协议生效之日可用的分处理方名单，SAP 也可以应客户请求提供该名单，其中包括 SAP 用来提供云服务的各个分处理方的名称、地址和角色。

6.2 New Subprocessors. SAP's use of Subprocessors is at its discretion, provided that:
新的分处理方。SAP 自行决定分处理方的使用，但前提是：

(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
SAP 应通过电子邮件或由 SAP 支持部门在提供的支持门户上发布的方式，提前通知客户分处理方名单的增加或更换情况，其中应列出新的分处理方的名称、地址和角色；以及

(b) Customer may object to such changes as set out in Section 6.3.
客户可根据第 6.3 节规定，对此类变更提出异议。

6.3 Objections to New Subprocessors.
对新的分处理方提出异议。

(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.
如客户依据数据保护法有合理理由反对新的分处理方处理个人数据，客户可通过向 SAP 发出书面通知终止协议（仅限于拟用新的分处理方的云服务）。此类终止应在客户作出决定之时生效，不得晚于自 SAP 向客户发出通知告知其新的分处理方起三十（30）天。如客户未在此三十（30）天期限内终止，即视为客户已接受新的分处理方。

(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.

在自 SAP 向客户发出通知告知其新的分处理方起的三十（30）天期限内，客户可请求双方共同诚意探讨异议的解决方案。此类探讨不得延长终止期限，也不影响 SAP 在三十（30）天期限后使用新的分处理方的权利。

(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.
本节（第 6.3 节）下的任何终止均应视为任何一方均无过错，并且应遵循协议条款。

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.
紧急更换。在变更原因超出 SAP 合理控制范围，因安全原因或其他紧急原因需要及时更换时，SAP 可在不提前发出通知的情况下更换分处理方。这种情况下，SAP 应在更换分处理方后尽快通知客户分处理方的更换。第 6.3 节将予以适用。

7. INTERNATIONAL PROCESSING
全球性处理

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.
全球性处理的条件。在数据保护法允许的情况下，SAP 有权依据本 DPA，在客户所在国家/地区之外处理个人数据，包括采用分处理方处理个人数据。

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:
标准合同条款。若 (i) 位于 EEA 或瑞士境内的控制方，其个人数据在 EEA、瑞士之外，以及欧盟确认能够依据 GDRP 第 45 条提供充足数据保护级别的安全国家/地区之外的任何国家/地区、组织或地域进行处理，或者若 (ii) 另一控制方的个人数据在全球范围内进行处理，且此类全球性处理需要依据控制方所在国家/地区的法律采取充分措施，且所需的充分措施可通过签订标准合同条款来实现，那么：

(a) SAP and Customer enter into the Standard Contractual Clauses;
SAP 与客户签订标准合同条款；

(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
客户与相关分处理方按如下其中一种模式签订标准合同条款：(i) 客户加入 SAP 或 SAP SE 与作为权利和义务独立所有人的分处理方之间签订的标准合同条款（以下简称“加入模式”），或者 (ii) 分处理方（由 SAP 代表）与客户签订标准合同条款（以下简称“授权委托模式”）。如果 SAP 通过第 6.1(c)节下提供的分处理方名单或向客户发送通知，明确确认分处理方适用于授权委托模式，则应采用授权委托模式，以及/或者

(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.

由客户依据协议授权使用云服务的其他控制方也可以根据上文第 7.2(a)和(b)节规定，采用与客户相同的方式与 SAP 和/或相关分处理方签订标准合同条款。此类情况下，客户将代表其他控制方签订标准合同条款。

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.

标准合同条款与协议的关系。存在冲突条款时，协议中任何条款的效力均不得视为高于标准合同条款。为避免疑义，本 DPA 在第 5 节和第 6 节中进一步规定了审计和分处理方规则，此类规定在涉及标准合同条款时同样适用。

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.

标准合同条款的管辖法律。标准合同条款应受相关控制方所在国家/地区的相关法律的管辖。

8. DOCUMENTATION; RECORDS OF PROCESSING

文档；处理记录

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.

各方负责遵守文档要求，尤其是在数据保护法要求时，维护处理记录。各方应合理协助另一方遵守文档要求，包括通过另一方合理请求的方式（如使用电子系统）提供另一方需要从其处获得的信息，支持另一方遵守与维护处理记录相关的任何义务。

9. EU ACCESS

EU 访问

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. If agreed in the Order Form for the eligible Cloud Service expressly identified there as being subject to EU Access, SAP shall provide the Cloud Service solely for production instances in accordance with this Section 9. Where EU Access is not agreed in the Order Form, this Section 9 shall not apply.

可选服务。EU 访问属于可由 SAP 提供的可选服务。若订购单中约定适用云服务明确指定为适用 EU 访问，SAP 应根据本节（第 9 节）仅为生产实例提供云服务。若订购单中没有约定 EU 访问，本节（第 9 节）将不适用。

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 访问。SAP 仅使用欧洲分处理方提供访问云服务中个人数据所需的支持，且 SAP 不得在 EEA 或瑞士地区之外导出个人数据，除非客户针对具体情况以书面形式（允许使用电子邮件方式）明确授权；或者根据第 9.4 节排除。

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.

数据中心位置。自协议生效之日起，用于托管云服务中个人数据的数据中心位于 EEA 或瑞士境内。未经客户事先书面同意（允许使用电子邮件方式），SAP 不得将客户实例迁移到 EEA 或瑞士境外的数据中心。如 SAP 计划将客户实例迁移到 EEA 或瑞士境内的数据中心，SAP 应就此在不晚于计划迁移日期之前的三十（30）天内，书面通知客户（允许使用电子邮件的方式）。

9.4 Exclusions. The following Personal Data is not subject to 9.2 and 9.3:
例外情形。以下个人数据不适用于第 9.2 节和第 9.3 节：

(a) Contact details of the sender of a support ticket; and
支持消息发送方的详细联系信息；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.
客户在填写支持消息时提交的任何其他个人数据。在填写支持消息时，客户可以选择不传输个人数据。如此数据为事件管理流程所必需的数据，则客户可以选择在将任何事件消息传输至 SAP 之前，对个人数据进行匿名处理。

10. DEFINITIONS
定义

Capitalized terms not defined herein will have the meanings given to them in the Agreement.
本协议中未定义的术语，应适用协议中对其赋予的含义。

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.
"控制方"是指独立或与其他方一起确定个人数据处理目的和方式的自然人、法人、公共机构、代理机构或其他团体；就本 DPA 而言，若客户作为另一控制方的处理方，对于 SAP，该客户应视为具有本 DPA 下相应控制方权利和义务的额外独立控制方。

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.
"数据中心"是指为数据中心所在区域内的客户托管云服务生产实例的位置，具体位置发布于：http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html 或已告知客户或在订购单中另行约定。

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).
"数据保护法"是指旨在保护个人基本权利、自由以及与依据协议处理个人数据相关的隐私权的适用法律（就双方之间的关系而言，若 SAP 代表客户处理个人数据，无论个人数据是否遵循 GDPR，均包括作为最低标准的 GDPR）。

10.4 "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.
"数据当事人"是指根据数据保护法规定，已识别或可识别的自然人。

10.5 "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.
"EEA"是指欧洲经济区，即欧盟成员国及冰岛、列支敦斯登和挪威。

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

"欧洲分处理方" 是指在 EEA 或瑞士境内以物理方式处理个人数据的分处理方。

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).

"个人数据" 是指受数据保护法保护的、与数据当事人有关的任何信息。就本 DPA 而言，仅包括以下个人数据：(i) 客户或其授权用户在使用云服务过程中输入或产生的个人数据，或 (ii) 为提供协议中所述的相关支持提供给 SAP 或其分处理方或者 SAP 或其分处理方访问的个人数据。个人数据是客户数据的组成部分（详见协议中的规定）。

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.

"个人数据违规" 是指确认的 (1) 意外或非法破坏、丢失、篡改、未经授权披露或第三方未经授权访问个人数据，或 (2) 涉及个人数据的类似事件。在以上每种情况下，控制方需要根据数据保护法的要求，向主管数据保护机构或数据当事人发送通知。

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.

"处理方" 是指代表控制方处理个人数据的自然人、法人、公共机构、代理机构或其他团体，可以是控制方的直接处理方，也可以是代表控制方处理个人数据的处理方的间接分处理方。

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).

"标准合同条款"（有时亦称为"欧盟模式条款"）是指标准合同条款（处理方）或欧盟委员会发布的任何后续版本（应自动适用）。

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.

"分处理方" 是指 SAP 关联企业、SAP SE、SAP SE 关联企业以及 SAP、SAP SE、SAP SE 关联企业聘用的与云服务有关且根据本 DPA 处理个人数据的第三方。

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 和标准合同条款（如适用）之附录 1

Data Exporter
数据导出方
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.
数据导出方是租用云服务的客户，允许授权用户输入、修订、使用、删除或以其他方式处理个人数据。若客户还允许其他控制方使用云服务，这些其他控制方也是数据导出方。

Data Importer
数据导入方
SAP and its Subprocessors provide the Cloud Service that includes the following support:
SAP 及其分处理方提供包含下列支持的云服务：

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 关联企业通过位于以下地方的 SAP 办事处为云服务数据中心提供远程支持：德国的圣莱昂-罗特、印度及 SAP 运营/云服务交付部门员工所在的其他地方。支持包括：

- Monitoring the Cloud Service
  监控云服务
- Backup & restoration of Customer Data stored in the Cloud Service
  备份和恢复保存在云服务中的客户数据
- Release and development of fixes and upgrades to the Cloud Service
  发布和开发云服务补丁及升级
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
  监控、管理基础云服务架构和数据库并排除故障
- Security monitoring, network-based intrusion detection support, penetration testing
  监控安全性、支持检测网络入侵并执行渗透测试

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.
当客户因云服务不可用或者未按预期供某些或所有授权用户使用而提交支持消息时，SAP SE 关联企业应提供支持。SAP 在一个独立于云服务生产实例的追踪系统中，接听电话、执行基本的故障排除和处理支持消息。

Data Subjects
数据当事人
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.
除非数据导出方另有规定，否则，传输的个人数据涉及以下数据当事人：员工、订约方、业务伙伴或将个人数据存储在云服务中的其他个人。

Data Categories
数据类别
The transferred Personal Data transferred concerns the following categories of data:
传输的个人数据涉及以下数据类别：

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.
客户确定每个租用的云服务的数据类别。客户可以在云服务实施期间配置数据字段或以云服务中提供的其他方式进行配置。传输的个人数据通常涉及以下数据类别：姓名、电话号码、电子邮件地址、时区、地址数据、系统访问/使用/权限数据、公司名称、合同数据、发票数据以及授权用户输入云服务的任何应用程序特定数据，并且可能包括银行账户数据、信用卡或借记卡数据。

Special Data Categories (if appropriate)
特殊数据类别（如适用）
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.
传输的个人数据涉及以下特殊数据类别：见协议（包括订购单）（如有）。

Processing Operations / Purposes
处理操作/目的
The transferred Personal Data is subject to the following basic processing activities:
传输的个人数据限于下列基本处理活动：

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
  使用个人数据设置、操作、监控和提供云服务（包括运营支持和技术支持）
- provision of Consulting Services;
  提供咨询服务
- communication to Authorized Users
  与授权用户沟通
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
  在指定数据中心（多租户架构）存储个人数据
- upload any fixes or upgrades to the Cloud Service
  上传云服务的任何补丁或升级
- back up of Personal Data
  备份个人数据
- computer processing of Personal Data, including data transmission, data retrieval, data access
  个人数据的计算机处理，包括数据传输、数据检索、数据访问
- network access to allow Personal Data transfer
  网络访问，以支持个人数据传输
- execution of instructions of Customer in accordance with the Agreement.
  根据协议执行客户指令。

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

DPA 和标准合同条款（如适用）之附录 2 — 技术措施和组织措施

This Appendix 2 comprises two sets of technical and organizational measures ("TOMs"):
本附录 2 包括两组技术措施和组织措施：

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.
  第一组技术措施和组织措施 (最后一次更新于 2018 年 4 月，未有变更)：适用于所有的云服务，以下定义的第二组技术措施和组织措施服务除外。

- **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.
  第二组技术措施和组织措施：仅适用于第二组技术措施和组织措施服务。截至 2020 年 5 月 4 日，"第二组技术措施和组织措施服务"是指以下云服务：SAP Analytics Cloud，SAP SuccessFactors 和 SAP Cloud Platform。SAP 可不时从第二组技术措施和组织措施指定服务列表中删除某项云服务。在此情况下，该云服务将受第一组技术措施和组织措施之约束。

TOMs SET 1
第一组技术措施和组织措施

Last Updated: April 2018
最后一次更新于 2018 年 4 月

1. TECHNICAL AND ORGANIZATIONAL MEASURES
技术措施和组织措施

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.
以下内容规定了 SAP 目前采用的技术措施和组织措施。SAP 可随时更改这些措施，且无需另行发送通知，但前提是维持相当或更高的安全等级。各项措施可由具有相同作用的新措施替代，但不得降低个人数据保护的安全等级。

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.
物理访问控制。未经授权的人员不得擅自进入处理和/或使用个人数据的数据处理系统所在的办公地、建筑物或房间。

Measures:
措施：

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
  SAP 基于 SAP 安全政策采用相应的措施保护其资产和设施
- In general, buildings are secured through access control systems (e.g., smart card access system).
  通常，采用门禁系统（如智能卡门禁系统）保障建筑物的安全。
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
  作为最低要求，建筑物最外层的入口必须安装认证密钥系统，包括现代的动态密钥管理。

- 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.
  根据安全等级，可采用其他措施进一步保护建筑物、个别区域和周围场所的安全。这些措施包括特定访问配置文件、视频监控、入侵报警系统以及生物识别门禁系统。
- 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.
  访问权限会依据系统和数据访问控制措施授予获得授权的个人（参见下文第 1.2 节和 1.3 节）。该措施同样适用于访客访问。进入 SAP 楼宇的来宾和访客必须在接待处登记姓名，而且必须由 SAP 授权员工陪同。
- SAP employees and external personnel must wear their ID cards at all SAP locations.
  SAP 员工和外部员工在所有 SAP 场所都必须佩带自己的身份卡。

Additional measures for Data Centers:
针对数据中心的其他措施：

- 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.
  所有数据中心都应遵守严格的安全流程，安装防护装置、监控摄像头、移动探测器，建立门禁机制并采取其他措施，从而保护设备和数据中心设施免受安全威胁。仅授权代表有权访问数据中心设施中的系统和基础架构。为保障数据中心的正常运行，会定期对物理安全设备（如移动传感器、摄像头等）进行维护。
- 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 和所有第三方数据中心提供商都会记录进入数据中心中 SAP 专属区域的授权人员的姓名和时间。

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.
系统访问控制。必须防止未经授权使用提供云服务的数据处理系统。

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
  按多个权限级别授予访问敏感系统的权限，包括存储和处理个人数据的该类系统。权限根据 SAP 安全政策通过定义的流程加以管理
- All personnel access SAP's systems with a unique identifier (user ID).
  所有人员使用唯一标识（用户标识）访问 SAP 的系统。
- 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 设定相应程序，确保只依照 SAP 安全政策（例如，未经授权不授予任何权限）执行请求的权限变更。如人员离开公司，其访问权限会被撤销。
- 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 已制定禁止共享密码的密码政策，用于管辖密码泄漏后的响应操作，以及要求定期更改密码和更改默认密码。分配个性化用户标识进行身份验证。所有密码都必须满足最低指定要求并以加密形式存储。例如，对于域密码，系统会按复杂密码的要求，强制每六（6）个月更改一次密码。每台计算机都有一个密码保护屏保。

- The company network is protected from the public network by firewalls.
  公司网络通过防火墙与公共网络隔离。
- 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 在公司网络的接入点（针对电子邮件帐户）和所有文件服务器及所有工作站中使用最新的杀毒软件。
- 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.
  实施安全补丁管理，定期部署相关安全更新。通过严格的身份验证确保对 SAP 公司网络和关键基础架构全面远程访问的安全。

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.
数据访问控制。有权使用数据处理系统的人员只能访问有权访问的个人数据，且未经授权不得在处理、使用和存储期间读取、复制、修改或删除个人数据。

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.
  作为 SAP 安全政策的一部分，个人数据至少需要达到 SAP 信息分类标准中与“保密”信息同等的保护级别。
- 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.
  本着需者方知的原则授予访问个人数据的权限。员工有权访问履行其职责所需的信息。SAP 采用权限概念，说明授予流程和各账户分配的角色（用户标识）。依照 SAP 安全政策保障所有客户数据的安全。
- 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.
  在数据中心或安全服务器机房中操作所有生产服务器。定期检查安全措施，保护处理个人数据的应用程序。为此，SAP 对其 IT 系统执行内部和外部安全检查和渗透测试。
- SAP does not allow the installation of software that has not been approved by SAP.
  SAP 不允许安装未经 SAP 批准的软件。
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
  SAP 安全标准规定如何删除或销毁不再需要的数据和数据载体。

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).

数据传输控制。除根据协议提供云服务所必需以外，不得在传输期间未经授权读取、复制、修改或删除个人数据。物理运输数据载体时，在 SAP 内部实施适当的措施（例如，加密和密闭容器）以提供约定的服务级别。

Measures:

措施：

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  依照 SAP 安全政策保护通过 SAP 内部网络传输的个人数据。
- 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).
  在 SAP 与其客户之间传输数据时，双方商定针对所传输个人数据的保护措施并将之纳入相关协议。这一点同样适用于物理数据传输和网络数据传输。在任何情况下，客户均对从 SAP 控制系统外传输的任何数据（如从 SAP 数据中心的防火墙外传输的数据）负责。

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.

数据输入控制。可执行追溯性检查和确定是否已在 SAP 数据处理系统中输入、修改或删除个人数据，并检查和确定执行此类操作的人员。

Measures:

措施：

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
  SAP 只允许授权人员根据需要在履行职责的过程中访问个人数据。
- 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.
  在技术可行的范围内，SAP 已就 SAP 或其分处理方对云服务中个人数据的输入、修改、删除或冻结实施记录系统。

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.

作业控制。委托处理的个人数据（即代表客户处理的个人数据）完全依据协议和客户的相关指令进行处理。

Measures:

措施：

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 采用控制和流程，确保遵守 SAP 与其客户、分处理方或其他服务提供商之间签署的合同。
- 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.
  作为 SAP 安全政策的一部分，个人数据至少需要达到 SAP 信息分类标准中与"保密"信息同等的保护级别。
- 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 员工和合同分处理方或其他服务提供商均受合同约束，遵守所有敏感信息（包括 SAP 客户和合作伙伴的商业秘密）的保密性。

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

可用性控制。避免意外或未经授权销毁或丢失个人数据。

Measures:

措施：

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
  SAP 采用定期备份流程，确保在必要时快速恢复关键业务系统。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
  SAP 使用不间断电源（如，UPS、电池、发电机等）确保数据中心的电力供应。
- 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 针对关键业务流程制定了业务应急计划，并为关键业务服务提供灾难恢复战略，详见文档或相关云服务的订购单中所述。
- Emergency processes and systems are regularly tested.
  定期测试紧急流程和系统。

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

数据分离控制。对出于不同目的收集的个人数据进行分开处理。

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 利用所部署软件的技术功能（如，多租户或单独系统架构）实现来自不同客户的个人数据的分离。
- Customer (including its Controllers) has access only to its own data.
  客户（包括其控制方）只能访问自己的数据。
- 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.
  如需用个人数据处理客户的支持事件，数据将被分配到该特定消息并仅用于处理该消息；如用于处理其他任何消息，则无法访问此数据。该数据存储在专用的支持系统中。

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

数据完整性控制。在处理活动中确保个人数据不受损、完整和实时。

Measures:

措施：

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

SAP 实施了多层防护战略，防止出现未经授权修改数据的行为。

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

SAP 特别采取了以下措施来实施上文所述的控制和措施。特别是：

- Firewalls;
  防火墙；
- Security Monitoring Center;
  安全监控中心；

- Antivirus software;
  杀毒软件；
- Backup and recovery;
  备份与恢复；
- External and internal penetration testing;
  内外部渗透测试；
- Regular external audits to prove security measures.
  定期外部审计以验证安全措施。

TOMs SET 2
第二组技术措施和组织措施

(*applies to TOMs Set 2 Services defined above*)
（适用于以上定义的第二组技术措施和组织措施服务）

Last Updated: May 4, 2020
最后一次更新于 2020 年 5 月 4 日

1. TECHNICAL AND ORGANIZATIONAL MEASURES
技术措施和组织措施

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.
以下内容规定了 SAP 目前采用的技术措施和组织措施。SAP 可随时更改这些措施，且无需另行发送通知，但前提是维持相当或更高的安全等级。各项措施可由具有相同作用的新措施替代，但不得降低个人数据保护的安全等级。

1.1 Physical Access Control.
物理访问控制。

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
  SAP 基于 SAP 安全政策采用相应的措施保护其资产和设施
- In general, buildings are secured through access control systems (e.g., smart card access system).
  通常，采用门禁系统（如智能卡门禁系统）保障建筑物的安全。
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
  作为最低要求，建筑物最外层的入口必须安装认证密钥系统，包括现代的动态密钥管理。
- 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.
  根据安全等级，可采用其他措施进一步保护建筑物、个别区域和周围场所的安全。这些措施包括特定访问配置文件、视频监控、入侵报警系统以及生物识别门禁系统。
- 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.
  访问权限会依据系统和数据访问控制措施授予获得授权的个人（参见下文第 1.2 节和 1.3 节）。该措施同样适用于访客访问。进入 SAP 楼宇的来宾和访客必须在接待处登记姓名，而且必须由 SAP 授权员工陪同。
- SAP employees and external personnel must wear their ID cards at all SAP locations.
  SAP 员工和外部员工在所有 SAP 场所都必须佩带自己的身份卡。

Additional measures for Data Centers:
针对数据中心的其他措施：

- 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.
  所有数据中心都应遵守严格的安全流程，安装防护装置、监控摄像头、移动探测器，建立门禁机制并采取其他措施，从而保护设备和数据中心设施免受安全威胁。仅授权代表有权访问数据中心设施中的系统和基础架构。为保障数据中心的正常运行，会定期对物理安全设备（如移动传感器、摄像头等）进行维护。

- 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 和所有第三方数据中心提供商都会记录进入数据中心中 SAP 专属区域的授权人员的姓名和时间。

1.2 System Access Control.
系统访问控制。

- 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.
  按多个权限级别授予访问敏感系统的权限，包括存储和处理个人数据的该类系统。权限根据 SAP 安全政策通过定义的流程加以管理。
- All personnel access SAP's systems with a unique identifier (user ID).
  所有人员使用唯一标识（用户标识）访问 SAP 的系统。
- 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 已有相应政策，旨在规定未经授权不授予任何权限，以及规定如人员离开公司，其访问权限会被撤销。
- 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 已制定禁止共享密码的密码政策，用于管辖密码泄漏后的响应操作，以及要求定期更改密码和更改默认密码。分配个性化用户标识进行身份验证。所有密码都必须满足最低指定要求并以加密形式存储。例如，对于域密码，系统会按复杂密码的要求，强制每六（6）个月更改一次密码。每台计算机都有一个密码保护屏保。
- The company network is protected from the public network by firewalls.
  公司网络通过防火墙与公共网络隔离。
- 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 在公司网络的接入点（针对电子邮件帐户）和所有文件服务器及所有工作站中使用最新的杀毒软件。
- Security patch management processes to deploy relevant security updates on a regular and periodic basis.
  安全补丁管理流程，以定期部署相关安全更新。
- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication.
  通过身份验证确保对 SAP 公司网络和关键基础架构全面远程访问的安全。

1.3 Data Access Control.
数据访问控制。

- 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.
  作为 SAP 安全政策的一部分，个人数据至少需要达到 SAP 信息分类标准中与“保密”信息同等的保护级别。
- 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.
  本着需者方知的原则授予访问个人数据的权限。员工有权访问履行其职责所需的信息。SAP 采用权限概念，说明授予流程和各账户分配的角色（用户标识）。依照 SAP 安全政策保障所有客户数据的安全。
- 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.

在数据中心或安全服务器机房中操作所有生产服务器。定期检查安全措施，保护处理个人数据的应用程序。为此，SAP 对其 IT 系统执行内部和外部安全检查和(或)渗透测试。

- Processes and policies to detect the installation of unapproved software on production systems.
  检测生产系统上未经批准软件的安装的流程和政策。
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
  SAP 安全标准规定如何删除或销毁不再需要的数据和数据载体。

1.4 Data Transmission Control.
数据传输控制。

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  依照 SAP 安全政策保护通过 SAP 内部网络传输的个人数据。
- 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).
  在 SAP 与其客户之间传输数据时，双方商定针对所传输个人数据的保护措施并将之纳入相关协议。这一点同样适用于物理数据传输和网络数据传输。在任何情况下，客户均对从 SAP 控制系统外传输的任何数据（如从 SAP 数据中心的防火墙外传输的数据）负责。

1.5 Data Input Control.
数据输入控制。

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
  SAP 只允许授权人员根据需要在履行职责的过程中访问个人数据。
- 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.
  在技术可行的范围内，SAP 已在大多数情况下就 SAP 或其分处理方对云服务中个人数据的输入、修改、删除或冻结实施记录系统。

1.6 Job Control.
作业控制。

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 采用控制和流程，确保遵守 SAP 与其客户、分处理方或其他服务提供商之间签署的合同。
- 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.
  作为 SAP 安全政策的一部分，个人数据至少需要达到 SAP 信息分类标准中与“保密”信息同等的保护级别。
- 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 员工和合同分处理方或其他服务提供商均受合同约束，遵守所有敏感信息（包括 SAP 客户和合作伙伴的商业秘密）的保密性。

1.7 Availability Control.
可用性控制。

SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
SAP 采用定期备份流程，确保在必要时快速恢复关键业务系统。

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

SAP 使用不间断电源（如，UPS、电池、发电机等）确保数据中心的电力供应。

- 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 针对关键业务流程制定了业务应急计划，并为关键业务服务提供灾难恢复战略，详见文档或相关云服务的订购单中所述。
- Emergency processes and systems are regularly tested.
  定期测试紧急流程和系统。

1.8 Data Separation Control.
数据分离控制。

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 利用所部署软件的技术功能（如，多租户或单独系统架构）实现来自不同客户的个人数据的分离。

- Customer (including its Controllers) has access only to its own data.
  客户（包括其控制方）只能访问自己的数据。
- 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.
  如需用个人数据处理客户的支持事件，数据将被分配到该特定消息并仅用于处理该消息；如用于处理其他任何消息，则无法访问此数据。该数据存储在专用的支持系统中。

1.9 Data Integrity Control.
数据完整性控制。

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

SAP 实施了多层防护战略，防止出现未经授权修改数据的行为。

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

SAP 特别采取了以下措施来实施上文所述的控制和措施。特别是：

- Firewalls;
  防火墙；
- Security Monitoring Center;
  安全监控中心；
- Antivirus software;
  杀毒软件；
- Backup and recovery;
  备份与恢复；
- External and internal penetration testing and/or regular external external audits to prove security measures.
  内外部渗透测试和（或）定期外部审计以验证安全措施。

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 和标准合同条款（如适用）之附录 3

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.
下表列出了 GDPR 的相关条款和 DPA 的对应条款，仅作说明之用。

Article of GDPR **GDPR 条款**	**Section of DPA** **DPA 小节**	**Click on link to see Section** **单击链接查看相关小节**
28(1)	2 and Appendix 2 2 和附录 2	Security of Processing and Appendix 2, Technical and Organizational Measures. Security of Processing 和附录 2，技术措施和组织措施。
28(2), 28(3) (d) and 28 (4) 28(2)、28(3) (d)和 28 (4)	6	SUBPROCESSORS SUBPROCESSORS
28 (3) sentence 1 28 (3)第 1 句	1.1 and Appendix 1, 1.2 1.1 和附录 1、1.2	Purpose and Application. Structure. Purpose **and Application.** Structure**.**
28(3) (a) and 29 28(3) (a)和 29	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)	3.3	Personnel. Personnel
28(3) (c) and 32 28(3) (c)和 32	2 and Appendix 2 2 和附录 2	Security of Processing and Appendix 2, Technical and Organizational Measures. Security of Processing 和附录 2，技术措施和组织措施。
28(3) (e)	3.4	Cooperation. Cooperation**.**
28(3) (f) and 32-36 28(3) (f)和 32-36	2 and Appendix 2, 3.5, 3.6 2 和附录 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 和附录 2，技术措施和组织措施。Personal **Data Breach Notification.** Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion Data export and Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS SUBPROCESSORS
30	8	Documentation; Records of processing Documentation; Records of processing
46(2) (c)	7.2	Standard Contractual Clauses Standard Contractual Clauses

Appendix 4 (FALLBACK)
附录 4（备用）

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]
标准合同条款（处理方）[2]

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
根据欧盟指令 95/46/EC 第 26(2)条（或在 2018 年 5 月 25 日后，法案 2016 年第 79 号第 44 条起），向成立于无法确保充分数据保护的第三方国家/地区的处理方传输个人数据的规定

Customer also on behalf of the other Controllers
也代表其他控制方的客户
(in the Clauses hereinafter referred to as the '**data exporter'**)
（在以下条款中统称为“**数据导出方**”）

and
和

SAP
(in the Clauses hereinafter referred to as the **'data importer'**)
（在以下条款中统称为**“数据导入方”**）

each a 'party'; together 'the parties',
以上各方分别称为“一方”，合称为“双方”，

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.
为就数据导出方向数据导入方传输附件 1 中规定的个人数据在隐私保护和个人基本权利和自由方面提供充分的保护，已达成如下合同条款（以下统称“条款”）：

Clause 1
第 1 条

Definitions
定义

For the purposes of the Clauses:
就条款而言：

(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

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

[2]根据2010年2月5日的委员会决议（2010/87/EU）

protection of individuals with regard to the processing of personal data and on the free movement of such data;

‘个人数据’、‘特殊数据类别’、‘处理/进行处理’、‘控制方’、‘处理方’、‘数据当事人’和‘监管部门’均适用欧洲议会和理事会于 1995 年 10 月 24 日通过的关于涉及个人数据处理的个人保护以及此类数据自由传输的 95/46/EC 指令中为其规定的含义；

(b) ‘the data exporter’ means the controller who transfers the personal data;

‘数据导出方’是指传输个人数据的控制方；

(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;

‘数据导入方’是指同意接收数据导出方的个人数据并在传输之后根据数据导出方的指令和条款项代其处理此类数据的处理方，该处理方所在的第三方国家/地区体系不受 95/46/EC 指令第 25(1)条规定的确保提供充分的数据保护的制约。

(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;

‘分处理方’是指数据导入方或数据导入方的任何其他分处理方委托的任何处理方，此类处理方同意从数据导入方或数据导入方的任何其他分处理方处接收个人数据，以专门用于在传输完成后根据数据导入方的指令、条款项和书面分包合同条款代其执行处理活动；

(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;

‘适用的数据保护法’是指保护个人基本权利和自由的法律，特别是适用于数据导出方成立所在欧盟成员国中的数据控制方且与个人数据处理相关的隐私权。

(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.

‘技术和组织安全措施’是指避免个人数据遭受意外或非法破坏或意外丢失、篡改、擅自披露或访问（特别是处理过程涉及网络数据传输的情况）以及其他非法形式的处理而采取的措施。

Clause 2
第 2 条

Details of the transfer
传输详细信息

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
传输详细信息，特别是特殊的个人数据类别（若适用），将在附件 1 中加以详细说明，并构成条款不可或缺的一部分。

Clause 3
第3条

Third-party beneficiary clause
第三方受益人条款

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.

数据当事人可以要求数据导出方作为第三方受益人履行本条款、第4(b)至(i)条、第5(a)至(e)和(g)至(j)条、第6(1)和(2)条、第7条、第8(2)条以及第9至12条。

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.

若数据导出方已实际消失或在法律上已不复存在，数据当人事可以要求数据导入方履行本条款、第5(a)至(e)和(g)条、第6条、第7条、第8(2)条以及第9至12条，除非任何后继实体已经根据合同或依法承担了数据导出方的全部法律义务，因此数据导出方的权利和义务将由该实体承担，在此情况下，数据当事人可以要求该实体履行上述条款。

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.

若数据导出方和数据导入方均已实际消失或在法律上已不复存在或已破产，数据当人事可以要求分处理方履行本条款、第5(a)至(e)和(g)条、第6条、第7条、第8(2)条以及第9至12条，除非任何后继实体已经根据合同或依法承担了数据导出方的全部法律义务，因此数据导出方的权利和义务将由该实体承担，在此情况下，数据当事人可以要求该实体履行上述条款。分处理方的此类第三方责任应限于其依据上述条款自己执行的处理操作。

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.

若数据当事人表达明确意愿且在国家法律允许的范围内，双方均不反对由协会或其他团队代表数据当事人。

Clause 4
第4条

Obligations of the data exporter
数据导出方的义务

The data exporter agrees and warrants:

数据导出方同意并保证：

(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;

一直并将继续依据适用数据保护法的相关规定处理个人数据（包括传输本身）（且在适用情况下，已就此通知数据导出方成立所在的欧盟成员国的相关机构）且不会违反该国的相关规定；

(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;

其已责成并在处理个人数据的整个过程中将责成数据导入方仅代表数据导出方依据适用的数据保护法和条款处理传输的个人数据；

(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;

数据导入方将就本合同附件 2 中规定的技术和组织安全措施提供充分的担保；

(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;

在评估适用数据保护法的要求之后，通过采取合适的安全措施保护个人数据免遭意外或非法破坏或意外丢失、篡改、擅自披露或访问（特别是处理过程涉及网络数据传输的情况）以及一切其他非法形式的处理，同时根据数据处理产生的风险以及要保护的数据的性质并考虑实施的先进技术和成本，采取上述措施，保证安全级别；

(e) that it will ensure compliance with the security measures;

确保遵守安全措施；

(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;

若传输涉及特殊数据类别，则应提前通知或在传输开始之前或在传输结束之后尽快通知数据当事人，告知其数据可能传输至无法提供 95/46/EC 指令规定的充分的数据保护的第三方国家/地区；

(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;

若数据导出方决定继续传输或解除暂停，依据第 5(b)条和第 8(3)条的规定将从数据导入方或任何分处理方处收到的通知转发给数据保护监管机构；

(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;

根据要求，应向数据当事人提供条款（除附件 2 外）副本和安全措施的概要说明以及须依据本条款提供的分处理服务的任何合同副本，除非条款或合同包含商业信息，在此情况下，可将此类商业信息从中删除；

(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

依据条款规定，在分处理情况下，处理活动将依据第 11 条由至少提供与数据导入方对个人数据采取同等保护和数据当事人权利的分处理方执行；及

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

确保遵守第 4(a)至(i)条款；

Clause 5

第 5 条

Obligations of the data importer

数据导入方的义务

The data importer agrees and warrants:

数据导入方同意并保证：

(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;

仅代表数据导出方依据其指令和条款处理个人数据；若数据导入方因故无法满足此类合规要求，则其同意就此及时通知数据导出方，在此情况下，数据导出方有权暂停数据传输和/或终止合同；

(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;

数据导入方没有理由认为对其适用的法律会阻止其履行从数据导出方处收到的指令及其在合同项下的义务；若该法律发生变更，且此类变更可能会对条款规定的担保和义务产生重大不利影响，则其在了解到此类变更时应及时通知数据导出方，在此情况下，数据导出方有权暂停数据传输和/或终止合同；

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

在处理传输的个人数据之前，其已实施附件 2 中规定的技术和组织安全措施；

(d) that it will promptly notify the data exporter about:

其将就以下情况及时通知数据导出方：

(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;

执法机构有关个人数据披露的任何具有法律约束力的请求，除非有其他禁止规定，如刑法为保护执法调查的机密性的禁止规定；

(ii) any accidental or unauthorised access; and

任何意外或未经授权访问个人数据的行为；及

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

数据当事人直接提出且未作出响应的任何请求，除非已获得相应的授权；

(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;

及时合理地处理数据导出方有关其传输后的个人数据处理的所有查询，并遵循监管机构就处理传输数据给出的相关建议；

(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;

根据数据导出方的请求，提交其数据处理设施以审核条款项下规定的处理活动，该审核程序应由数据导出方或者数据导出方指定的检验机构执行；检验机构应由独立成员组成，拥有所需的专业资格并承担保密职责，同时在适用的情况下，与监管机构达成协议；

(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;

若数据当事人无法从数据导出方处获取条款副本或有关分处理的任何现有合同副本，根据请求，数据导入方将向数据当事人提供上述副本，除非条款或合同中包含商业信息，在此情况下，可将附件 2 的此类商业信息从中删除，且应以安全措施的概要描述替代附件 2；

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

就分处理情况，其先前已通知数据导出方并获得数据导出方的事先书面同意；

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

分处理方将依据第 11 条执行处理活动；

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

及时向数据导出方发送依据条款达成的任何分处理方协议副本。

Clause 6
第6条

Liability
责任

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.

双方同意，因任何一方或分处理方未履行第 3 条或第 11 条中规定的义务而遭受损害的任何数据当事人，均有权获得数据导出方就此类损害给予的赔偿。

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.

因数据导出方已实际消失或在法律上不复存在或已破产的事实导致数据当事人无法依据第 1 款规定就数据导入方或其分处理方未履行第 3 条或第 11 条规定的义务向数据导出方索要赔偿的，数据导入方同意数据当事人将其视为数据导出方对其提出索赔，除非任何后继实体根据合同或依法承担了数据导出方的全部法律义务，在此情况下，数据当事人可以对该实体实施其相关权利。

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
数据导入方不得依赖分处理方未履行义务的行为来规避自己的责任。

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.

因数据导出方和数据导入方已实际消失或在法律上不复存在或已破产的事实导致数据当事人无法依据第 1、2 款的规定就分处理方未履行第 3 条或第 11 条规定的义务向数据导出方或数据导入方索要赔偿的，数据分处理方同意数据当事人将其视为数据导出方或数据导入方就其条款项下的处理操作对其提出索赔，除非任何后继实体根据合同或依法承担了数据导出方或数据导入方的全部法律义务，在此情况下，数据当事人可以对该实体实施其相关权利。分处理方的责任应限于其依据条款自己执行的处理操作。

Clause 7
第7条

Mediation and jurisdiction
调解和司法管辖

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:
数据导入方同意，若数据当事人提出第三方受益人权利请求且/或依据条款索要损失赔偿，则数据导入方将接受数据当事人的以下决定：

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
将纠纷提交给独立个人或（若适用）监管机构进行调解；

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
将纠纷提交给数据导出方所在成员国的法庭；

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.
双方同意，数据当事人所做的选择不会损害其依据国家法律或国际法律的其他规定寻求补救措施的实质性或程序性权利。

Clause 8
第8条

Cooperation with supervisory authorities
配合监管机构

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.
数据导出方同意根据监管机构的要求或适用数据保护法的规定向监管机构送存本合同的副本。

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.
双方同意，监管机构有权对数据导入方及任何分处理方进行审计，且审计范围和条件与适用数据保护法针对数据导出方执行审计应用的范围和条件相同。

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).
数据导入方应及时通知数据导出方适合其或任何分处理方的现行法律，避免依据第2款的规定对数据导入方或任何分处理方进行审计。在此情况下，数据导出方应有权采取第5(b)条中的预见性措施。

Clause 9
第9条

Governing law
管辖法律

The Clauses shall be governed by the law of the Member State in which the data exporter is established.
条款应受数据导出方所在成员国法律的管辖。

Clause 10
第10条

Variation of the contract
合同变更

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.
双方承诺不会更改或修改合同条款。在不与已有条款相抵触的前提下，根据需要，双方可以增加有关业务相关问题的条款。

Clause 11
第11条

Sub-processing
分处理

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.

依据条款规定，未经数据导出方事先书面同意，数据导入方不得分包其代表数据导出方执行的任何处理操作。若数据导入方分包其在条款项下的义务且已征得数据导出方的同意，则其仅应通过与分处理方签订书面协议的方式进行分包，依据该协议，要对分处理方强制执行本条款项下数据导入方所应承担的同等义务。若分处理方未能履行其在该等书面协议项下的数据保护义务，则数据导入方应全权负责分处理方在该等协议项下的义务履行。

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.

数据导入方和分处理方之间先前签署的书面合同还应就以下情形提供第 3 条规定的第三方受益人条款：因数据导出方或数据导入方实际消失或在法律上不复存在或已破产的事实而导致数据当事人无法对数据导出方或数据导入方提出第 6 条第 1 款中提及的赔偿要求，且未有后继实体根据合同或依法承担数据导出方或数据导入方的全部法律义务。分处理方的此类第三方责任应限于其依据上述条款自己执行的处理操作。

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.

第 1 段中提及的与合同分处理的数据保护事宜有关的规定应受数据导出方所在成员国法律的管辖。

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.

数据导出方应保存一份依据条款达成的且由数据导入方依据第 5(j)条规定予以通知的分处理协议清单，该清单应至少每年更新一次。该清单应提交给数据导出方的数据保护监管机构。

Clause 12
第12 条

Obligation after the termination of personal data-processing services
终止个人数据处理服务后的义务

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.

双方同意，在终止提供数据处理服务之后，数据导入方和分处理方应根据数据导出方的决定向数据导出方返还所传输的全部个人数据及其副本或者销毁全部个人数据并向数据导出方出示相关证明，除非依据相关法律，数据导入方不得返还或销毁所传输的全部或部分个人数据。在此情况下，数据导入方保证，其将保证所传输个人数据的保密性，且不再主动处理所传输的个人数据。

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.

数据导入方和分处理方保证，其将根据数据导出方和/或监管机构的请求提交数据处理设施，以进行第 1 款所述的措施审核。