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.
目的。

This document is a data processing agreement ("**DPA**") between SAP and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Cloud Service. It states the technical and organizational measures SAP uses to protect Personal Data that is stored in the production system of the Cloud Service.
本文档为 SAP 与客户之间签订的数据处理协议（以下简称"**DPA**"），适用于客户和各个数据控制方就云服务使用提供的个人数据。本文档规定了 SAP 用于保护存储在云服务生产系统中的个人数据的技术措施和组织措施。

1.2 Application of the Standard Contractual Clauses Document.
适用标准合同条款文档。

If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.
个人数据的处理涉及国际传输时，按照第 5 节的规定适用标准合同条款，且标准合同条款以引用形式纳入本协议。

1.3 Governance.
管辖。

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use the Cloud Service to the terms of this DPA.
除非第 5.2 节另有规定，否则客户全权负责管理来自其他数据控制方的所有请求。客户负责约束其允许根据本 DPA 条款使用云服务的任何其他数据控制方。

2. APPENDICES
附录

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in the Cloud Service. Appendix 1 states the details of the processing SAP will provide via the Cloud Service. Appendix 2 states the technical and organizational measures SAP applies to the Cloud Service, unless the Agreement states otherwise.
客户及其数据控制方确定收集和处理云服务中存储的个人数据的目的。附录 1 规定 SAP 将通过云服务进行的具体处理操作。附录 2 规定 SAP 对云服务采用的技术措施和组织措施，协议另有规定的除外。

3. SAP OBLIGATIONS
SAP 的义务

3.1 Instructions from Customer.
客户的指令。

SAP will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Cloud Service. SAP may correct or remove any Personal Data in accordance with the Customer's instruction. If SAP cannot comply with an instruction, it will promptly notify Customer (email permitted).
SAP 应遵循客户（代表自身或代表其数据控制方）就个人数据所发出的指令，但指令属于以下情况的除外：(i) 为法律所禁止或 (ii) 要求对云服务进行实质变更。SAP 可根据客户的指令更正或删除任何个人数据。若 SAP 无法遵从某项指令，应立即通知客户（允许使用电子邮件的方式）。

3.2 Data Secrecy.
数据保密。

To process Personal Data, SAP and its Subprocessors will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law. SAP and its

Subprocessors will regularly train individuals having access to Personal Data in data security and data privacy measures.
处理个人数据时，SAP 及其分处理方应仅采用有义务依据数据保护法遵守数据保密和通信保密的人员。SAP 及其分处理方应定期对获得个人数据访问权限的员工进行数据安全和数据隐私措施方面的培训。

3.3 Technical and Organizational Measures.
技术措施和组织措施。

(a) SAP will use the appropriate technical and organizational measures stated in Appendix 2.
SAP 应采用附录 2 中规定的相应技术措施和组织措施。

(b) Appendix 2 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.
附录 2 适用于云服务生产系统。客户不得在非生产环境中存储任何个人数据。

(c) SAP provides the Cloud Service to SAP's entire customer base hosted out of the same data center and receiving the same Cloud Service. Customer agrees SAP may improve the measures taken in Appendix 2 in protecting Personal Data so long as it does not diminish the level of data protection.
SAP 为托管于相同数据中心并接收相同云服务的整个 SAP 客户群提供云服务。客户同意，SAP 可以改进附录 2 中规定的个人数据保护措施，但前提是不能降低数据保护等级。

3.4 Security Breach Notification.
安全违规通知。

SAP will promptly inform Customer if it becomes aware of any Security Breach.
如 SAP 发现任何安全违规行为，将立即通过客户。

3.5 Cooperation.
合作。

At Customer's request, SAP will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data.
如客户请求，SAP 应给予客户或任何数据控制方合理的支持，协助其处理数据当事人或监管部门就 SAP 对个人数据的处理提出的要求。

4. SUBPROCESSORS
分处理方

4.1 Permitted Use.
许可使用。

(a) Customer and Data Controllers authorize SAP to subcontract the processing of Personal Data to Subprocessors. SAP is responsible for any breaches of the Agreement caused by its Subprocessors.
客户和数据控制方授权 SAP 将个人数据处理分包给分处理方。SAP 应对其分处理方违反协议的任何行为承担责任。

(b) Subprocessors will have the same obligations as SAP does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.
作为数据处理方（或分处理方），分处理方在个人数据处理方面与 SAP 拥有相同义务。

(c) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, SAP will regularly evaluate each Subprocessor's security practices as they relate to data handling.
在选择分处理方之前，SAP 应评估分处理方的安全、隐私和保密实践。分处理方可以提供安全认证，证明其采用了相应的安全措施。若未提供，SAP 应定期评估每个分处理方在数据处理方面的安全实践。

(d) If Customer requests, SAP will inform Customer of the name, address and role of each Subprocessor it uses to provide the Cloud Service.
若客户要求，SAP 应告知客户其用于提供云服务的每个分处理方的名称、地址和角色。

4.2 New Subprocessors.
新的分处理方。

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

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

SAP 应以电子邮件或在支持门户上发布的方式提前通知客户对生效之日已有的分处理方清单的任何变更（"紧急更换"或未更换情况下删除分处理方的情况除外）。

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

如客户有合理的理由质疑分处理方的个人数据处理，客户可以在收到 SAP 通知后的三十（30）日内向 SAP 发出书面通知，反对 SAP 使用某个分处理方。如客户反对使用某个分处理方，双方应共同诚意探讨解决方案。SAP 可以选择：(i) 不使用某个分处理方，或 (ii) 采取客户在其反对声明中要求的纠正措施，然后再使用该分处理方。如上述选项均无法合理实现，且客户仍以合理理由提出反对意见，则任何一方均可在发出书面通知的三十（30）日内终止协议。如客户未在收到通知的三十（30）日内提出反对意见，即视为客户已接受新的分处理方。

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

如客户的反对声明在发出的六十（60）日内仍未得到解决，且 SAP 未收到任何终止通知，即视为客户已接受分处理方。

4.3 Emergency Replacement.
紧急更换。

SAP may change a Subprocessor where the reason for the change is outside of SAP's reasonable control. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).
在变更原因超出 SAP 合理控制范围的情况下，SAP 可更换分处理方。这种情况下，SAP 应尽快通知客户分处理方的更换。客户保留其依据第 4.2(b)节反对更换分处理方的权利。

5. INTERNATIONAL TRANSFERS
国际传输

5.1 Limitations on International Transfer.
国际传输限制。

Personal Data from an EEA or Swiss Data Controller(s) may only be exported or accessed by SAP or its Subprocessors outside the EEA or Switzerland (**"International Transfer"**):
在以下前提条件下，来自 EEA 或瑞士数据控制方的个人数据才能由 SAP 或其分处理方导出到 EEA 或瑞士境外或者在 EEA 或瑞士境外进行访问（以下简称**"国际传输"**）：

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

接收方或者接收方处理或访问个人数据所在的国家或地域可确保达到欧盟委员会确定的充分的保护级别，能够在个人数据的处理过程中确保数据当事人的权利和自由；或

(b) in accordance with Section 5.2.
符合第 5.2 节的规定。

5.2 Standard Contractual Clauses and Multi-tier Framework.
标准合同条款和多层框架。

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

如某个国家/地区的国际传输不能确保达到欧盟委员会确定的充分的保护级别，无法在个人数据的处理过程中确保数据当事人的权利和自由，则适用标准合同条款。

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

对于第三方国家/地区分处理方，SAP 已经在分处理方处理个人数据之前签署了未变更版本的标准合同条款。客户（自身并代表各数据控制方）特此同意接受 SAP 与第三方国家/地区分处理方签署的标准合同条款。如数据保护法未提供直接执行权利，SAP 应代表数据控制方要求分处理方执行此类标准合同条款。

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

存在冲突条款时，本 DPA 中任何条款的效力均不得视为高于标准合同条款。

6. CERTIFICATIONS AND AUDITS
认证和审计

6.1 Customer Audits.
客户审计。

Customer or its independent third party auditor may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:
在以下情况下，客户或其独立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：

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

SAP 未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 认证报告。一旦客户请求，SOC 审计报告或 ISO 证书应通过第三方审计机构或 SAP 提供；

(b) A Security Breach has occurred;
已出现安全违规；

(c) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this DPA;
客户或其他数据控制方有合理理由怀疑 SAP 未履行本 DPA 中规定的义务；

(d) An audit is formally requested by Customer's or another Data Controller's data protection authority; or
客户或其他数据控制方的数据保护机构正式要求实施审计；或者

(e) Mandatory Data Protection Law provides Customer with a direct audit right.
强制性数据保护法为客户提供直接审计权利。

Where Customer audits SAP's environment, SAP will reasonably support Customer in its audit processes.
若客户要审计 SAP 环境，SAP 应在审计过程中为客户提供合理支持。

6.2 Audit Restrictions.
审计限制。

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

客户审计在任意十二（12）个月期限内仅限执行一次，审计时间最多三（3）个工作日，审计范围由双方提前合理约定。需要至少提前六（6）天发出合理通知，除非数据保护法要求尽早实施审计。SAP 和客户应利用现有的证书或其他审计报告最大限度减少重复审计工作。客户和 SAP 自行承担各自的审计费用，除非客户依据第 6.1 (c)节（除非此类审计发现 SAP 违约，这种情况下，SAP 应自行承担审计费用）、6.1 (d)节或 6.1 (e)节进行审计。这几种情况下，客户自行承担费用和开展审计所需的 SAP 内部资源的成本。如审计发现 SAP 违反其在本协议下的义务，SAP 应自担费用立即对违规行为进行补救。

7. EU ACCESS
EU 访问

7.1 Optional Service.
可选服务。

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

如包含在订购单中，SAP 同意为第 7 节（本节）规定的适用云服务提供 EU 访问。

7.2 EU Access.
EU 访问。

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

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。

7.3 Data Center Location.
数据中心位置。

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

自订购单生效之日起，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 不会将客户实例迁移到 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天内，书面通知客户（允许使用电子邮件的方式）。

7.4 Exclusions.
例外情形。

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

以下个人数据不受第 7.2-7.3 节的约束：

(a) Contact details of the sender of a support ticket;
支持消息发送方的详细联系信息；

(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；

(c) Personal Data in non-production systems.
非生产系统中的个人数据。

8. 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。 **"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。

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

"数据控制方"是指独立或与他人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。

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

"数据处理方"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。

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

"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。

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

"数据当事人"是指已识别或可识别的自然人。

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

8.7 **"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。

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

"个人数据"在本 DPA 中是指与数据当事人相关的任何信息，仅包括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。此外，还包括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 或其分处理方可访问的个人数据。个人数据是客户数据的组成部分。

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

"安全违规"是指确认的 (1) 意外或非法破坏、丢失、篡改、披露客户个人数据或保密数据，或 (2) 适用法律要求数据处理方向数据控制方发送通知且涉及个人数据的类似事件。

8.10 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. They include Appendices 1 and 2 attached to this DPA.

"标准合同条款"或有时亦称为"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）。现行标准合同条款位于 http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc。这些条款包括随附于本 DPA 的附录 1 和 2。

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

"分处理方"是指 SAP 或 SAP 关联企业聘用的用于处理个人数据的 SAP 关联企业和第三方。

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

"第三方国家/地区分处理方"是指位于 EEA 境外以及欧盟委员会针对其发布适当决议的国家/地区境外的任何分处理方，决议详见 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm。

Appendix 1 to Data processing agreement and Standard Contractual Clauses
数据处理协议和标准合同条款附录 1

Data Exporter
数据导出方
The Data Exporter subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.
租用云服务的数据导出方，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。

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 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 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 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 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 Order Form, if any.

传输的个人数据涉及以下特殊数据类别：见订购单（如有）。

Processing Operations

处理操作

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 this Agreement
  根据本协议执行客户指令

Appendix 2 – Technical and Organizational Measures
附录 2 — 技术措施和组织措施

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

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

以下各节定义了 SAP 的当前安全措施。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。这可能意味着，各项措施会由具有相同作用的新措施替换而不降低安全等级。

1.1 Physical Access Control.
物理访问控制。

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

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 a security classification conducted by an internal security department.
  SAP 会基于内部安全部门划定的安全等级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 ensure 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。为保证数据中心的正常运行，应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 persons 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 专属区域的人员姓名和时间。

1.2 System Access Control.
系统访问控制。

Data processing systems used to provide the SAP Services must be prevented from being used without authorization.
必须防止未经授权使用提供 SAP 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. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
  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。落实流程以确保授权用户具备添加、删除或修改用户的相应权限。
- All users access SAP's systems with a unique identifier (user ID).
  所有用户使用唯一标识（用户标识）访问 SAP 的系统。
- SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
  SAP 设定相应程序以确保只依照准则（例如，未经授权不授予任何权限）执行请求的权限变更。如用户离开公司，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 ensure regular and periodic deployment of relevant security updates.
  实施安全补丁管理，确保定期部署相关安全更新。
- Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.
  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 .
数据访问控制。

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

有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, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards. Confidential information must be processed confidentially.
  本着需者方知的原则授予访问个人、保密或敏感信息的权限。换言之，员工或外部第三方可以访问完成工作所需的信息。SAP 采用权限概念，说明分配权限的方式以及所分配的权限及对象。依照 SAP 安全政策和标准保护所有个人、保密或其他敏感数据。保密信息必须以保密方式进行处理。
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
  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、保密或其他敏感信息的应用程序。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 personal software or other software that has not been approved by SAP.
  SAP 不允许安装未经 SAP 批准的个人软件或其他软件。
- 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.
数据传输控制。

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).
除根据相关服务协议提供服务所必需以外，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）以确保达到约定的服务级别。

- Personal Data transfer over SAP internal networks are protected in the same manner as any other confidential data according to SAP Security Policy.
  依据 SAP 安全政策，通过 SAP 内部网络传输的个人数据将接受任何其他保密数据同等的保护。
- 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。

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.

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 persons to access Personal Data as required in the course of their work.
  SAP 只允许授权人员根据需要在他们的工作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 SAP's Products and Services to the fullest extent possible.
  在 SAP 产品和服务支持的最大范围内，SAP 已就 SAP 或其分处理方对个人数据的输入、修改、删除或冻结实施记录系统。

1.6 Job Control.
作业控制。

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer.
委托处理的个人数据（即代表客户处理的个人数据）完全依据相关协议和客户的相关指令进行处理。

Measures:

措施：

- SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 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。
- For on premise support services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge or full active participation of the customer.
  对于企业预置型支持服务，SAP 提供专门指定的安全支持消息设施，SAP 在其中为传输访问数据和密码提供特殊的访问控制和监控安全区域。SAP 客户始终对其远程支持连接具有控制权。不了解客户或未得到客户全力积极支持的 SAP 员工不得访问客户系统。

1.7 Availability Control.
可用性控制。

Personal Data will be protected against accidental or unauthorized destruction or loss.
避免意外或未经授权销毁或丢失个人数据。

Measures:

措施：

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
  SAP 采用备份流程和其他措施确保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 ensure 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 contingency plans as well as business and disaster recovery strategies for the provided Services.
  SAP 针对提供的服务制定了应急计划以及业务和灾难恢复战略。
- 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。

Personal Data collected for different purposes can be processed separately.
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。
- Customers (including their Affiliates) have access only to their own data.
  客户（包括其关联企业）只能访问自己的数据。
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.
  如需用个人数据处理特定客户的支持事件，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。

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