PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES
SAP クラウドサービスに関する個人データ処理契約書

1. BACKGROUND
1. 背景
1.1 Purpose.
1.1 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.
本書は、顧客と SAP 間におけるデータ処理契約書（以下「DPA」）であり、顧客及び各「データコントローラー」により、その「クラウドサービス」の利用に関連して提供される個人データに適用される。本書では、「クラウドサービス」の本稼動システム内に格納される「個人データ」を保護するために SAP が用いる技術的及び組織的な対策を記載する。
1.2 Application of the Standard Contractual Clauses Document.
1.2 標準契約条項文書の適用。
If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.
「個人データ」の処理に「国際移転」がかかわる場合は、第 5 条に記載するとおり「標準契約条項」が適用され、参照により組み込まれる。
1.3 Governance.
1.3 ガバナンス。
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.
第 5.2 条に規定する場合を除き、顧客は、他の「データコントローラー」からのすべての要求の管理に単独で責任を負う。顧客は、他の「データコントローラー」に「クラウドサービス」の利用を認める場合は、本 DPA の条項に拘束せしめるものとする。

2. APPENDICES
2. 付属書
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.
顧客及びその「データコントローラー」は、「クラウドサービス」内の「個人データ」の収集及び処理の目的を決定する。「付属書 1」に、SAP が「クラウドサービス」を介して提供する処理の詳細を記載する。「付属書 2」に、「本契約」に別段の記載がある場合を除き、SAP が「クラウドサービス」に適用する技術的及び組織的な対策を記載する。

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

SAP は、「個人データ」に関して顧客から（顧客自身に代わり若しくはその「データコントローラー」に代わって）受けた指示に従うものとする。ただし、それが（i）法的に禁止されている、又は（ii）「クラウドサービス」に対する重大な変更を必要とするものである場合は、その限りではない。SAP は、顧客の指示に従って、「個人データ」を修正又は削除することができるものとする。SAP が指示に従うことができない場合は、速やかに顧客に通知するものとする（電子メールも認められる）。

3.2 Data Secrecy.

3.2 データの秘密性。

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.

「個人データ」を処理するため、SAP 及びその「処理外注先」は、「データ保護法」に基づいてデータ及び通信の秘密性を守る義務を有する職員のみを使用するものとする。SAP 及びその「処理外注先」は、データセキュリティ及びデータプライバシーの対策において、「個人データ」へのアクセス権を有する個人に対して定期的に研修を行うものとする。

3.3 Technical and Organizational Measures.

3.3 技術的及び組織的対策。

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

(a) SAP は、「付属書 2」に記載する適切な技術的及び組織的な対策を用いるものとする。

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

(b) 「付属書 2」は、「クラウドサービス」の本稼動システムに適用される。顧客は、いかなる「個人データ」も非本稼動環境には格納しないこと。

(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.

(c) SAP は、「クラウドサービス」を、同一のデータセンターからホストされ、同一の「クラウドサービス」を受けている SAP の全顧客ベースに提供する。顧客は、「個人データ」の保護において講じる「付属書 2」の対策を、それがデータ保護のレベルを低下させるものでない限り、SAP が改善できることに同意する。

3.4 Security Breach Notification.

3.4 セキュリティ侵害の通知。

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

SAP は、「セキュリティ侵害」があったことを認知した場合、速やかに顧客に通知するものとする。

3.5 Cooperation.

3.5 協力。

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.

顧客の求めに応じて、SAP は、SAP による「個人データ」の処理に関する「データ主体」又は規制当局からの要求への対応において、顧客又は「データコントローラー」に合理的な範囲でサポートを行うものとする。

4. SUBPROCESSORS

4. 処理外注先

4.1 Permitted Use.

4.1 許可される使用。

(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.

(a) 顧客と「データコントローラー」は、SAP が「個人データ」の処理を「処理外注先」に外注することを承認する。SAP は、その「処理外注先」による「本契約」の違反があった場合はその責任を負う。

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

(b) 「処理外注先」は、自らが「個人データ」を処理することに関して、SAP が「データ処理業者」（又は「処理外注先」）として有するのと同じ義務を有するものとする。

(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.

(c) SAP は、選定に先立ち、「処理外注先」のセキュリティ、プライバシー、及び秘密保持の実務を評価するものとする。「処理外注先」は、その適切なセキュリティ対策の使用を証する、セキュリティ認定資格を有している場合がある。有していない場合、SAP は、データの扱いに関連する各「処理外注先」のセキュリティに関する実務を、定期的に評価するものとする。

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

(d) 顧客が要請する場合、SAP は、「クラウドサービス」の提供のために使用する「処理外注先」の名称、住所、及び役割について顧客に通知するものとする。

4.2 New Subprocessors.

4.2 新規の処理外注先。

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

SAP による「処理外注先」の使用はその裁量で行うが、以下を条件とする。

(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).

(a) SAP は、「発効日」において用意されている「処理外注先」のリストに変更があれば、事前に顧客に通知（電子メールで、又は「サポートポータル」での掲示により）するものとする（「緊急交代」又は交代なしでの「処理外注先」の削除の場合を除く）。

(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.

(b) 「処理外注先」による「個人データ」の処理に関連する正当な理由が顧客にある場合、顧客は、SAP からの通知の受領後 30 日以内に書面で SAP に通知することにより、SAP による「処理外注先」の使用に異議を唱えることができるものとする。顧客が「処理外注先」の使用に異議を唱えた場合、両当事者は、誠意をもって会合を持ち、解決策を協議するものとする。SAP は、（i）その「処理外注先」を使用しない、又は（ii）顧客がその異議において要求した是正措置をとり、その「処理外注先」を使用する、のいずれかを選択できるものとする。これら選択肢のいずれも合理的に可能ではなく、顧客が引き続き正当な理由で異議を唱える場合は、いずれの当事者も、30 日前までの書面による通知を以て「本契約」を解除できるものとする。通知の受領後 30 日以内に顧客が異議を唱えなかった場合、顧客は、新たな「処理外注先」を承認したものとみなされる。

(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.

(c) 顧客の異議がそれが唱えられた後 60 日間未解決のままであり、かつ SAP が解除の通知を受領しなかった場合、顧客は、その「処理外注先」を承認するものとみなされる。

4.3 Emergency Replacement.

4.3 緊急交代。

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

SAP は、変更の理由が SAP の合理的な支配を超えたものである場合、「処理外注先」を変更できるものとする。この場合、SAP は、代替となる「処理外注先」について、可及的速やかに顧客に通知するものとする。顧客は、第 4.2 条（b）に基づいて、代替となる「処理外注先」に対して異議を唱える権利を保持する。

5. INTERNATIONAL TRANSFERS

5. 国際移転

5.1 Limitations on International Transfer.

5.1 国際移転に関する制限事項。

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

EEA 又はスイスの「データコントローラー」からの「個人データ」は、以下を条件としてのみ、SAP 又はその「処理外注先」により EEA 又はスイスの域外に輸出できるものとする（以下「**国際移転**」）。

(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

(a) 受領者側、又は受領者が「個人データ」の処理又はアクセスを行う国若しくは地域が、「個人データ」の処理に関連して、欧州委員会により判断されるところの「データ主体」の権利と自由の保護に関する十分な水準を確保している場合、又は

(b) in accordance with Section 5.2.

(b) 第 5.2 条に従っている。

5.2 Standard Contractual Clauses and Multi-tier Framework.

5.2 標準契約条項及び複数階層の枠組み。

(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.

(a) 「個人データ」の処理に関連して、欧州委員会により判断されるところの「データ主体」の権利と自由の保護に関する十分な水準が確保されていない国への「国際移転」が行われる場合は、「標準契約条項」が適用される。

(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.

(b) 「第三国の処理外注先」に関しては、SAP は、当該「処理外注先」による「個人データ」の処理に先立ち、変更のないバージョンの「標準契約条項」を締結している。顧客はここに（自らが並びに各「データコントローラー」に代わり）、SAP と「第三国の処理外注先」間における「標準契約条項」に同意する。「データ保護法」に基づいて直接の実施権が行使できない場合、SAP は、「データコントローラー」に代わって「標準契約条項」を「処理外注先」に強制するものとする。

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

(c) 本 DPA のいずれの定めも、「標準契約条項」の相反する条項に優先するとは解釈されないものとする。

6. CERTIFICATIONS AND AUDITS

6. 認証及び監査

6.1 Customer Audits.

6.1 顧客の監査。

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:

顧客とその独立した第三者の監査人は、以下のいずれかの場合にのみ、SAP が処理する「個人データ」に関連する管理環境及びセキュリティの実務を監査することができるものとする：

(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;

(a) SAP が、次のいずれかを提出することにより、「クラウドサービス」の本稼動システムを保護する技術的及び組織的な対策への準拠の十分な証拠を提供していない：（i）ISO 27001 又はその他の標準への準拠に関する認定資格（当該証明書に記載された範囲）、又は（ii）有効な ISAE3402 及び/若しくは ISAE3000 認証報告書。顧客の要請に応じて、第三者の監査人又は SAP を通じて、SOC 監査報告書又は ISO 証明書が入手できる。

(b) A Security Breach has occurred;

(b) 「セキュリティ侵害」が発生した。

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

(c) SAP が本 DPA に基づく義務を遵守していないことを、顧客又は別の「データコントローラー」が疑う合理的な根拠がある。

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

(d) 顧客又は別の「データコントローラー」のデータ保護当局から、監査が正式に要求された。

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

(e) 強行法規である「データ保護法」により、顧客に直接的な監査の権利が与えられている。

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

顧客が SAP の環境を監査する場合、SAP はその監査プロセスにおいて合理的な範囲で顧客をサポートするものとする。

6.2 Audit Restrictions.

6.2 監査の制限事項。

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.

顧客による監査は、任意の 12 カ月間に 1 回を上限とし、期間は最長で 3 営業日に、また両当事者で事前に合理的な合意がなされた範囲に制限されるものとする。60 日以上前までの妥当な事前の通知を必要とするが、「データ保護法」によりそれより早期の監査が求められる場合はこの限りではない。顧客と SAP は、監査の繰り返しを最小限に抑えるため、現行の認定書又はその他の監査報告書を使用するものとする。顧客と SAP はそれぞれ、各自の監査の費用を負担するものとする。ただし、顧客が第 6.1 条（c）に基づいて監査を行う場合（当該の監査において

SAP による違反が発覚した場合を除く。その場合、SAP は自身の監査費用を負担するものとする）、第 6.1 条（d）又は第 6.1 条（e）に基づいて監査を行う場合はその限りではない。これらの場合、顧客は、自身の費用及び監査の実施に要した SAP の社内リソースのコストを負担するものとする。監査により SAP が「本契約」に基づくその義務に違反していることが判定された場合、SAP は当該の違反を自らの費用で速やかに是正するものとする。

7. EU ACCESS
7. EU アクセス

7.1 Optional Service.
7.1 オプションのサービス。

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

「注文書」に含まれている場合、SAP は、本第 7 条に記載するとおり、対象となる「クラウドサービス」について「EU アクセス」を提供することに同意する。

7.2 EU Access.
7.2 EU アクセス。

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

SAP は、「クラウドサービス」内で「個人データ」へのアクセスが必要なサポートの提供において、ヨーロッパの「処理外注先」のみを使用するものとする。

7.3 Data Center Location.
7.3 データセンターの所在地。

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.

「注文書発効日」において、「クラウドサービス」内で「個人データ」をホストするために使われる「データセンター」は、EEA 又はスイスに所在している。SAP は、顧客の事前の書面による同意（電子メールも認められる）なくして、顧客インスタンスを、EEA 又はスイスの国外にある「データセンター」に移行しないものとする。SAP が顧客インスタンスを EEA 又はスイス内のデータセンターに移行することを予定している場合、SAP は、予定する移行の 30 日前までに、書面で（電子メールも認められる）顧客に通知するものとする。

7.4 Exclusions.
7.4 除外規定。

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

以下の「個人データ」には、7.2 ～ 7.3 条の要件は適用されない。

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

(a) サポートチケットの送信元の連絡先の詳細。

(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;

(b) サポートチケットを申請する際に顧客から提出されたその他の「個人データ」。顧客は、サポートチケットを申請する際に、「個人データ」を送信しないことも選択できる。そのデータがインシデントの管理プロセスに必要な場合、顧客は、SAP にインシデントメッセージを送信する前に、当該「個人データ」を匿名化することもできる。

(c) Personal Data in non-production systems.

(c) 非本稼動システム内の「個人データ」。

8. DEFINITIONS

8. 定義

Capitalized terms not defined herein will have the meanings given to them in the Agreement. 本書で定義されていない鍵括弧付きの用語は、「本契約」に定める意味を有するものとする。

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

8.1 **「データセンター」**とは、顧客のために、その地域において「クラウドサービス」の本稼動インスタンスがホストされる場所をいい、 http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html で公表されるか、顧客に通知されるか、又は「注文書」で別途合意される。

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.

8.2 **「データコントローラー」**とは、自然人若しくは法人、公共団体、公的機関等、単独で又は他者と共同で、「個人データ」の処理の目的と手段を決定する主体をいう。

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.

8.3 **「データ処理業者」**とは、自然人若しくは法人、公共団体、公的機関等、コントローラーに代わって、個人データの処理を行う主体をいう。

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.

8.4 **「データ保護法」**とは、「本契約」に基づく「個人データ」の処理に関して、個人の基本的人権及び自由並びにそのプライバシーの権利を保護する、適用される法律をいう。

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

8.5 **「データ主体」**とは、特定された又は特定可能な自然人をいう。

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

8.6 **「EEA」**とは、ヨーロッパ経済領域、すなわち欧州連合の加盟国並びにアイスランド、リヒテンシュタイン及びノルウェーをいう。

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

8.7 **「欧州の処理外注先」**とは、EEA 又はスイスにおいて、「個人データ」を物理的に処理している「処理外注先」をいう。

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.

8.8 **「個人データ」**とは、本 DPA における「データ主体」に関連する情報をいい、顧客若しくはその「認定ユーザー」により「クラウドサービス」に入力された、又はそれらによる「クラウドサービス」の利用から派生した個人データのみが含まれる。また、SAP 又はその「処理外注先」により、「本契約」に基づくサポートを提供するために供された若しくはアクセスされた個人データも含まれる。「個人データ」は、「顧客データ」のサブセットである。

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.

8.9 **「セキュリティ侵害」**とは、確認された（1）顧客の「個人データ」若しくは「秘密データ」の偶発的若しくは違法な破壊、喪失、改変、若しくは開示、又は（2）適用法に基づいて「データ処理業者」が「データコントローラー」に通知を行う必要がある、「個人データ」が関わる同様の出来事をいう。

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.

8.10 **「標準契約条項」**（「EU モデル条項」と呼ばれる場合もある）とは、欧州委員会により発表される「標準契約条項（処理業者）」又はその後続版をいう（これは自動的に適用されるものとする）。現行の「標準契約条項」は、http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc に掲載されている。これには、本 DPA に添付された「付属書 1」及び「付属書 2」が含まれる。

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

8.11 **「処理外注先」**とは、個人データを処理するために SAP 又は SAP の「関連会社」が契約する「SAP 関連会社」及び第三者をいう。

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.

8.12 **「第三国の処理外注先」**とは、EEA 外並びに、欧州委員会が http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm で公開している、十分な保護が行われているとの決定を公表している国以外に法人格を有する「処理外注先」をいう。

Appendix 1 to Data processing agreement and Standard Contractual Clauses
データ処理契約及び標準契約条項に対する付属書 1

Data Exporter
データエクスポーター
The Data Exporter subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.
「認定ユーザー」が「個人データ」の入力、修正、使用、削除、又はその他処理を行うことを可能とする「クラウドサービス」に加入している、「データエクスポーター」。

Data Importer
データインポーター
SAP and its Subprocessors provide the Cloud Service that includes the following support:
SAP 及びその「処理外注先」は、以下のサポートを含む「クラウドサービス」を提供する。
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 関連会社」は、ザンクトレオン/ロート（ドイツ）、インド及びその他の「運用」/「クラウド提供」の業務で SAP が職員を雇用している場所にある SAP の施設からリモートで、「クラウドサービス」のデータセンターをサポートする。サポートには、以下が含まれる：

- Monitoring the Cloud Service
- クラウドサービスの監視
- Backup & restoration of Customer Data stored in the Cloud Service
- 「クラウドサービス」内に保存された「顧客データ」のバックアップ及び復元
- Release and development of fixes and upgrades to the Cloud Service
- 「クラウドサービス」に対する修正及びアップグレードのリリースと開発
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- 基礎をなす「クラウドサービス」のインフラストラクチャー及びデータベースの監視、トラブルシューティング及び管理
- Security monitoring, network-based intrusion detection support, penetration testing
- セキュリティ監視、ネットワークベースの侵入検知サポート、侵入テスト

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.
「SAP 関連会社」は、一部又は全部の「認定ユーザー」に対して「クラウドサービス」が利用できない又は期待どおりに機能しないことを理由に顧客がサポートチケットを発行した場合に、サポートを提供する。SAP は、電話に応対して基本的なトラブルシューティングを行うとともに、「クラウドサービス」の本稼動インスタンスとは分離されたトラッキングシステム内で、サポートチケットを処理する。

Data Subjects
データ主体
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.
「データエクスポーター」により別段の定めがある場合を除き、転送される「個人データ」は次のカテゴリーのデータ主体に関連する：「クラウドサービス」内に「個人データ」が保存されている従業員、契約者、取引先又はその他の個人。

Data Categories
データのカテゴリー
The transferred Personal Data transferred concerns the following categories of data:
転送される「個人データ」は、次のカテゴリーのデータに関連する：
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.
顧客は、加入している「クラウドサービス」ごとに、データのカテゴリーを決定する。顧客は、「クラウドサービス」の導入時に、又は「クラウドサービス」で定めるその他の方法でデータフィールドを設定することができる。転送される「個人データ」は一般的に、以下のカテゴリーに関連する：氏名、電話番号、電子メールアドレス、時間帯、住所情報、システムに関するアクセス/利用/権限情報、会社名、契約情報、請求情報、及び「認定ユーザー」が「クラウドサービス」に入力する、アプリケーション固有の情報（銀行口座情報、クレジットカード情報、又はデビットカード情報を含む場合がある）。

Special Data Categories (if appropriate)
特別なデータカテゴリー（該当する場合）
The transferred Personal Data concerns the following special categories of data: As set out in the Order Form, if any.
転送される「個人データ」は、次の特別なカテゴリーに関連する：「注文書」に定めるとおり（ある場合）。

Processing Operations
処理業務
The transferred Personal Data is subject to the following basic processing activities:
転送される「個人データ」は、以下の基本的な処理作業の対象となる：

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- 「クラウドサービス」のセットアップ、運用、監視及び提供を行うための「個人データ」の使用（「運用サポート」及び「テクニカルサポート」を含む）
- provision of Consulting Services;
- 「コンサルティングサービス」の提供
- communication to Authorized Users
- 「認定ユーザー」へのコミュニケーション
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)

- 専用の「データセンター」（マルチテナントアーキテクチャー）への「個人データ」の保存
- upload any fixes or upgrades to the Cloud Service
- 「クラウドサービス」の修正やアップグレードのアップロード
- back up of Personal Data
- 「個人データ」のバックアップ
- computer processing of Personal Data, including data transmission, data retrieval, data access
- 「個人データ」のコンピューター処理（データ伝送、データ検索、データアクセスを含む）
- network access to allow Personal Data transfer
- 「個人データ」の転送を可能にするためのネットワークアクセス
- execution of instructions of Customer in accordance with this Agreement
- 「本契約」に従って行う、顧客の指示の実行

Appendix 2 – Technical and Organizational Measures
付属書 2 – 技術的及び組織的対策

1. TECHNICAL AND ORGANIZATIONAL MEASURES
1. 技術的及び組織的対策

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.

以下の項では、SAP の現行のセキュリティ対策を定める。SAP は、同等以上のレベルのセキュリティを維持する限り、通知を行うことなく、随時これらを変更することができるものとする。これは、個々の対策が、セキュリティレベルを下げることなく、同様の目的を持った新規の対策で置き換えられる場合があることを意味する。

1.1 Physical Access Control.
1.1 物理的なアクセス制御。

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.

権限を有しない人物が、「個人データ」を処理及び/又は使用するデータ処理システムが配置された敷地、建物、又は部屋への物理的アクセスを得ることを防止する。

Measures:

対策：

- SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- SAP は、社内のセキュリティ部門が行うセキュリティ分類に基づく適切な手段を使用して、自身の資産及び施設を保護する。
- In general, buildings are secured through access control systems (e.g., smart card access system).
- 通常、建物はアクセス制御システム（スマートカードによるアクセスシステムなど）によりセキュリティ保護されている。
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- 最少要件として、建物の最も外側の入口部分には、認証を受けたキーシステム（最新の能動的なキー管理を含む）を取り付けなければならない。
- 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.
- セキュリティの分類に応じて、建物、各領域及び周囲の敷地が、追加的手段によってさらに保護される場合がある。これには、特定のアクセスプロファイル、ビデオ監視、侵入警報装置、及びバイオメトリクスによるアクセス制御システムが含まれる。
- 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.
- アクセス権は、「システム及びデータアクセス制御」対策（下記第 1.2 条及び第 1.3 条を参照）に従って、権限を有する人物に個別に付与される。これは、訪問者の立ち入りに対しても適用される。SAP の建物を訪れる来客及び訪問者については、受付で名前を登録し、権限を有する SAP の職員が付き添う必要がある。
- SAP employees and external personnel must wear their ID cards at all SAP locations.
- SAP の従業員及び外部の人員は、SAP のすべての場所で、自身の ID カードを身に付けていなければならない。

Additional measures for Data Centers:
データセンターに関する追加の対策：

- 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.
- すべての「データセンター」は、機器及び「データセンター」の施設が危険にさらされることを防止するために、警備員、監視カメラ、動作感知装置、アクセス制御手順及びその他手段によって実現される厳正なセキュリティ手順に従う。権限を有する担当者のみが、「データセンター」施設内のシステム及びインフラストラクチャーにアクセスすることができる。適切な機能性を維持するために、物理的なセキュリティ機器（動作感知装置、カメラなど）は、定期的な保守が行われる。
- 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 とすべての第三者「データセンター」プロバイダーは、「データセンター」内の SAP の部外者立ち入り禁止領域に入場した人物の名前及び時間を記録する。

1.2 System Access Control.

1.2 システムアクセス制御。

Data processing systems used to provide the SAP Services must be prevented from being used without authorization.
「SAP のサービス」の提供のために使用されるデータ処理システムでは、権限のない使用を防止しなければならない。

Measures:
対策：

- 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.
- 機密に関するシステム（「個人データ」の格納及び処理を行うシステムを含む）に対してアクセス権を付与する際は、複数の権限付与レベルが用いられる。ユーザーの追加、削除、又は修正について、認定ユーザーにしかるべき権限が付与されるようにするための手順が導入されている。
- All users access SAP's systems with a unique identifier (user ID).
- すべてのユーザーは、固有の識別情報（ユーザー ID）を使用して、SAP のシステムにアクセスする。
- 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 では、要請された権限の変更が、確実にガイドラインに従ってのみ実行されるようにする手続きが導入されている（たとえば、承認なしにいかなる権利も付与されないなど）。ユーザーが退職する場合、本人のアクセス権は取り消される。
- 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 では、パスワードの共有を禁じ、パスワードの開示に対する対応を定めるとともに、定期的にパスワードを変更しデフォルトのパスワードは変更することを要求する、パスワードポリシーを定めている。個人専用のユーザー ID が、認証のために割り当てられる。すべてのパスワードは定められた最小要件を満たしていなければならず、暗号化された形式で保存される。ドメインパスワードについては、システム

により、6 カ月ごとに、複雑なパスワードの要件に従ったパスワードの変更が義務付けられる。各コンピューターには、パスワードで保護されたスクリーンセーバーが備えられている。

- The company network is protected from the public network by firewalls.
- 会社のネットワークは、ファイアウォールにより、公共ネットワークから保護されている。
- 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 は、会社のネットワークに対するアクセスポイント（電子メールアカウント用）に加えて、すべてのファイルサーバー及びすべてのワークステーションで、最新のアンチウィルスソフトウェアを使用している。
- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- 関連するセキュリティアップデートの定期的なデプロイメントを確実にするために、セキュリティパッチ管理が導入されている。
- Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.
- SAP の企業ネットワーク及び重要なインフラストラクチャーへのフルリモートアクセスは、強力な認証によって保護されている。

1.3 Data Access Control .

1.3 データアクセス制御。

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.

データ処理システムの使用権限を有する個人は、アクセス権を有する「個人データ」のみを利用でき、処理、使用、及び保存の過程において、権限なしに「個人データ」が読み取り、コピー、修正、又は削除されることがあってはならない。

Measures:

対策：

- 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.
- SAP の「セキュリティポリシー」の一環として、「個人データ」には、SAP の「情報分類」基準に従って、少なくとも「秘密」情報と同じ保護レベルが必要である。
- 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.
- 個人情報、秘密情報、又は取り扱いに注意を要する情報へのアクセスは、知る必要を基準として認められる。すなわち、従業員又は外部の第三者は、自身の任務を完了するために必要な情報にアクセスすることができる。SAP は、権限が付与された方法、及びどの権限が誰に付与されたかについて記録する権限付与コンセプトを使用している。すべての個人情報、秘密情報、その他取り扱いに注意を要する情報は、SAP のセキュリティに関する方針及び標準に従って保護されている。秘密情報は、秘密を保って処理されなければならない。
- 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.
- すべての本稼動サーバーの稼動は、「データセンター」又はセキュリティ対策が施されたサーバールームで行われる。個人情報、秘密情報、又はその他取り扱いに注意を要する情報の処理を行うアプリケーショ

ンを保護するセキュリティ対策は、定期的にチェックが行われている。このため、SAP では、その IT システムについて、社内外のセキュリティチェック及び侵入テストを実施している。

- SAP does not allow the installation of personal software or other software that has not been approved by SAP.
- SAP では、SAP が承認していない個人のソフトウェア又はその他ソフトウェアのインストールを認めていない。
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
- SAP のセキュリティ基準では、データ及びデータ記憶媒体が不要となった場合に、それらを削除又は破壊する方法を定めている。

1.4 Data Transmission Control.

1.4 データ伝送制御。

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).

関連するサービス契約に従って「サービス」の提供に必要な場合を除き、「個人データ」は、転送時に権限なく読み取り、コピー、修正、又は削除を行ってはならない。データ記憶媒体が物理的に輸送される場合は、合意されたサービスレベルを確実にするために SAP において十分な対策が導入されている（たとえば、暗号化、鉛ライニングの施されたコンテナなど）。

- Personal Data transfer over SAP internal networks are protected in the same manner as any other confidential data according to SAP Security Policy.
- SAP の社内ネットワークにおける「個人データ」の伝送は、SAP の「セキュリティポリシー」に従って、その他の秘密情報と同様の方法で保護されている。
- 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).
- データが SAP とその顧客との間で転送される場合は、転送される「個人データ」の保護手段が相互に合意され、関連する「本契約」の一部となる。これは、物理的及びネットワークベースのデータ転送の両方に適用される。いずれの場合も、顧客は、SAP が管理するシステムの外部にデータがある場合は、そのデータ転送に責任を負う（データが、SAP の「データセンター」のファイアウォールの外に伝送される場合など）。

1.5 Data Input Control.

1.5 データ入力制御。

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.

「個人データ」が、SAP のデータ処理システムに入力された、修正された、又はそこから削除されたかどうか、及びそれを行ったのが誰かを、遡って調査し立証することが可能であるものとする。

Measures:

対策：

- SAP only allows authorized persons to access Personal Data as required in the course of their work.
- SAP は、権限を有する要員のみに、当該要員の任務の過程で必要な場合に限り「個人データ」にアクセスすることを認める。
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within SAP's Products and Services to the fullest extent possible.

- SAP は、可能な最大限度まで、SAP の「製品」及び「サービス」内での SAP 又はその「処理外注先」による「個人データ」の入力、修正、及び削除、又はブロックに対するロギングシステムを導入している。

1.6 Job Control.

1.6 ジョブ制御。

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.

委託により処理される「個人データ」（つまり、顧客の代行で処理される「個人データ」）は、専ら関連する契約及び顧客の関連した指示に従って処理される。

Measures:

対策：

- SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, subprocessors or other service providers.
- SAP は、自身とその顧客、処理外注先又はその他サービスプロバイダー間の契約の遵守を確実にするための、管理手段及び手順を使用する。
- 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.
- SAP の「セキュリティポリシー」の一環として、「個人データ」には、SAP の「情報分類」基準に従って、少なくとも「秘密」情報と同じ保護レベルが必要である。
- 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.
- SAP の従業員及び契約を結んでいる処理外注先又はその他のサービスプロバイダーはすべて、取り扱いに注意を要するすべての情報（SAP の顧客及びパートナーの営業秘密を含む）の守秘義務を遵守するべく、契約上で拘束される。
- 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.
- オンプレミスのサポートサービスについて、SAP は特別に指定された、セキュリティ対策が施されたサポートチケット施設を提供する。ここでは、アクセス情報及びパスワードの転送のために、アクセス管理及び監視された特別なセキュリティ領域が、SAP により提供される。SAP の顧客は、常時そのリモートサポート接続を管理する権限を有する。SAP の従業員は、顧客の知識又はその完全かつ積極的な関与なくして、顧客のシステムにアクセスすることはできない。

1.7 Availability Control.

1.7 可用性制御。

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

「個人データ」は、偶発的又は不正な破壊又は喪失から保護されるものとする。

Measures:

対策：

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- SAP は、必要に応じてかつ必要な場合に、業務上不可欠なシステムの迅速な回復を確実にする、バックアップ手順及びその他措置を講じる。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- SAP は、「データセンター」において電力を確実に利用可能とするため、無中断の電力供給（たとえば、UPS、バッテリー、発電機など）を使用する。

- SAP has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- SAP は、提供される「サービス」について、危機管理計画に加えて、事業及び災害復旧計画を定めている。
- Emergency processes and systems are regularly tested.
- 緊急対応の手順及びシステムについては、定期的に試験が行われる。

1.8 Data Separation Control.

1.8 データ分離制御。

Personal Data collected for different purposes can be processed separately.

異なる目的で収集された「個人データ」は、別々に処理することができる。

Measures:

対策：

- 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 は、配備されたソフトウェアの技術的機能（たとえば、マルチテナントや分離システムランドスケープ）を使用して、複数の顧客に由来する「個人データ」間のデータ分離を実現する。
- Customers (including their Affiliates) have access only to their own data.
- 顧客（その「関連会社」を含む）は、自身のデータのみにアクセスすることができる。
- 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.
- 「個人データ」が、特定の顧客からのサポートインシデントを処理するために必要な場合は、当該データはその特定のメッセージに割り当てられ、当該メッセージの処理のためにのみ使用される。その他のメッセージを処理するためにこのデータへのアクセスが行われることはない。このデータは、専用のサポートシステムに保存される。

1.9 Data Integrity Control .

1.9 データ完全性制御。

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

「個人データ」は、処理作業中、損なわれることなく、完全かつ最新の状態に保たれる。

Measures:

対策：

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

SAP は、権限外の修正に対する保護対策として、複数階層の防御戦略を導入している。

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

とりわけ、SAP では、以下を使用して上記の管理と対策のセクションを実施している。とりわけ、以下を指す。

- Firewalls;
- ファイアウォール
- Security Monitoring Center;
- セキュリティ監視センター
- Antivirus software;
- アンチウィルスソフトウェア
- Backup and recovery;
- バックアップ及び復元
- External and internal penetration testing;
- 外部及び内部の侵入テスト
- Regular external audits to prove security measures.
- セキュリティ対策を証明する定期的な外部監査