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 // 背景

1.1 **Purpose and Application.** This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments. **//** 目的及び適用 本書（以下「DPA」）は、「本契約」に組み込まれ、顧客と SAP 間の契約書（電子形式を含む）の一部を構成する。この DPA は、SAP 及びその「処理外注先」により、その「クラウドサービス」の提供に関連して処理される「個人データ」に適用される。この DPA は、「クラウドサービス」の非本稼動環境が SAP により提供される場合、かかる環境には適用されず、顧客は、かかる環境に「個人データ」を保存してはならない。

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. **//** 構造 「付属書 1」及び「付属書 2」がこの DPA に組み込まれ、その一部を構成する。それらの付属書では、合意された内容、処理の性質と目的、「個人データ」の種類、データ主体のカテゴリー、及び該当する技術的及び組織的対策を記載している。

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 と顧客は、「一般データ保護規則 2016/679」（以下「GDPR」）により「管理者」及び「処理業者」に課される要件、とりわけ GDPR の第 28 条及び第 32 条乃至第 36 条について、この DPA に基づいて処理される顧客/「管理者」の「個人データ」に適用される場合に、その範囲で同要件を確認して採用することがそれぞれの当事者の責任であることに合意する。参考までに、「付属書 3」に、関連する GDPR の要件及びこの DPA の対応するセクションを一覧にしている。

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 this 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 such other Controller/s as the Customer has permitted to use 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. **//** ガバナンス SAP は「処理業者」となり、顧客（及び「クラウドサービス」の使用を顧客が許可する事業体）は、この DPA に基づく「管理者」となる。顧客は単一の連絡窓口となり、この DPA に従って「個人データ」を処理することに対する、すべての関連する権限、同意及び許可を得ることに単独で責任を負う。これには、該当する場合、SAP を「処理業者」として使用することの、「管理者」による承認も含まれる。顧客が権限、同意、指示又は許可が顧客により提供した場合、それらは、顧客自身に代わってだけではなく、顧客が「クラウドサービス」を使用することを許可したその他の当該「管理者」にも代わって提供されるものとする。SAP が顧客に連絡又は通知した場合、かかる連絡又は通知は、「クラウドサービス」の使用を顧客により許可された「管理者」により受領されたとみなされ、顧客はかかる連絡及び通知を関連する「管理者」に転送する責任を負う。

1.5. The Act With Respect to the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the "Act"). Without limiting Customer's obligations to SAP under section 1.4 above, Customer and those entities that Customer permits to use the Cloud Service as Controllers under this DPA have complied with the obligations including, without limitation, obtaining the consent of all relevant Persons (as defined in the Act) with respect to the provision of Specific Personal Information (as defined in the Act) as may be required or directed under the Act, including, without limitation, Article 19. **//** 行政手続における特定の個人を識別するための番号の利用等に関する法律（「マイナンバー法」） 上記第 1.4 条に基づく顧客の SAP に対する義務を制限することなく、顧客及び顧客がこの DPA の下で「管理者」として「クラウドサービス」の利用を認めた事業体は、「特定個人情報」（「マイナンバー法」で定義）の提供に関連して必要とされる、関連する「本人」（「マイナンバー法」で定義）の同意の取得を含め、「マイナンバー法」第 19 条及びその他の規定における指示及び要求に従う。

2. SECURITY OF PROCESSING // 処理のセキュリティ

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data. **//** 適切な技術的及び組織的対策 SAP は、「付属書 2」に定める技術的及び組織的対策を導入しており、これを適用する。顧客は、かかる対策を確認しており、「注文書」において顧客が選択した「クラウドサービス」に関して、当該の対策が「個人データ」の処理の技術水準、導入のコスト、性質、範囲、背景及び目的を考慮に入れて適切であることに同意する。

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. **//** 変更 SAP は、「付属書 2」に定める技術的及び組織的対策を、同じ「データセンター」からホストされ、同じ「クラウドサービス」を受けている、SAP の全顧客ベースに適用する。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、「付属書 2」に定める対策を随時変更することができるものとする。個々の対策は、「個人データ」を保護するセキュリティレベルを損なわず同じ目的にかなう新たな対策に置き換えられる場合がある。

3. SAP OBLIGATIONS // SAP の義務

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted). **//** 顧客からの指示 SAP は、顧客からの文書による指示に従ってのみ、「個人データ」を処理する。「本契約」（この DPA を含む）は、かかる文書による初回の指示となり、「クラウドサービス」のそれぞれの使用は、さらなる指示となる。SAP は、それ以外の顧客の指示があった場合、それが「データ保護法」により求められ、技術的に可能であり、かつ「クラウドサービス」への変更を必要としない限り、従うべく合理的な努力を払う。前述の例外のいずれかが当てはまり、又は SAP がその他指示に従うことができない、若しくは指示が「データ保護法」に抵触するという見解である場合、SAP は直ちに顧客に通知する（電子メールも可）。

3.2 **Processing on Legal Requirement.** SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest. **//** **法的要求に基づく処理** SAP はまた、適用法により求められる場合も、「個人データ」を処理する場合がある。その場合、SAP は、処理を行う前に当該法的要件について顧客に連絡するものとする。ただし、公益の重要な理由によりかかる連絡が法律で禁止されている場合はその限りではない。

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. **//** **職員** 「個人データ」を処理するため、SAP 及びその「処理外注先」は、機密保持に関する確約を行った、権限のある職員にのみアクセス権を付与するものとする。SAP 及びその「処理外注先」は、該当する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職員に対して定期的に研修を行うものとする。

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. **//** **協力** 顧客の求めに応じて、SAP は、SAP による「個人データ」の処理又は「個人データ違反」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、顧客及び「管理者」に合理的な範囲で協力するものとする。SAP は、「個人データ」の処理に関連して「データ主体」から何らかの要求を受けた場合、（該当する場合は）顧客のさらなる指示なくしてかかる要求に自らが応えることなく、合理的な範囲で可及的速やかに顧客に通知するものとする。SAP は、「個人データ」の修正若しくは「クラウドサービス」からの「個人データ」の削除を行う、又は「データ保護法」に従ってその処理を制限する顧客の能力をサポートする機能を提供するものとする。かかる機能が提供されない場合、SAP は、顧客の指示及び「データ保護法」に従って「個人データ」の修正若しくは削除を行うか、又はその処理を制限するものとする。

3.5 **Personal Data Breach Notification.** SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP. **//** **個人データ違反の通知** SAP は、「個人データ違反」を認識した場合、遅滞なく顧客に通知するとともに、「データ保護法」に基づいて「個人データ違反」を報告する顧客の義務を顧客が達成することを支援するため、自身が保持する合理的範囲の情報を提供するものとする。SAP は、かかる情報を、入手可能となり次第段階的に提供することができるものとする。かかる通知は、SAP による過失又は責任の認容とは解釈されないものとする。

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. **//** **データ保護に関する影響評価** 「データ保護法」に従って、顧客（又はその「管理者」）がデータ保護に関する影響評価又は規制当局との事前協議を行う必要がある場合、顧客の求めにより、SAP は「クラウドサービス」に関して一般的に入手可能な文書を提供するものとする（たとえば、この DPA、「本契約」、監査の報告書や証明書など）。それ以外の支援については、両当事者間で相互に合意されるものとする。

4. DATA EXPORT AND DELETION // データのエクスポート及び削除

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. **//** **顧客によるエクスポート及び取り出し** 「サブスクリプション期間」中、「本契約」に従って、顧客は、随時「個人データ」にアクセスすることができる。顧客は、標準フォーマットで自身の「個人データ」をエクスポートし、取り出すことができる。エクスポートや取り出しには、技術的な制限がかかる場合があり、その場合顧客と SAP は、「個人データ」への顧客のアクセスを可能とするための合理的な方法を探求するものとする。

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. **//** **削除** 「サブスクリプション期間」が満了する前に、顧客は、SAP のセルフサービスエクスポートツール（利用できる場合）を使用して、「クラウドサービス」からの「個人データ」の最終的なエクスポートを実行することができる（その場合は「個人データ」の「返却」とみなされるものとする）。「サブスクリプション期間」の終了時、顧客は「本契約」によって、「データ保護法」に従った合理的な期間（6 カ月を超えない）内に、「クラウドサービス」をホストしているサーバー上に残存している「個人データ」を削除するよう SAP に指示する。ただし、適用法により保管が求められる場合はこの限りではない。

5. CERTIFICATIONS AND AUDITS // 認証及び監査

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: **//** **顧客による監査** 顧客又は SAP にとって合理的に受容可能な第三者の監査人（SAP の競合相手である、又は適切に資格を有しない若しくは独立的ではない第三者監査人は除外するものとする）は、以下の場合に限り、SAP が処理する「個人データ」に関連する SAP の管理環境及びセキュリティ実務の監査を行う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 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 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場合：(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 又はその他の SOC1-3 認証報告書。顧客の要請があれば、第三者の監査人又は SAP を通じて、監査報告書又は ISO 証明書を入手できる。

(b) A Personal Data Breach has occurred; **//** 「個人データ違反」が発生した場合

(c) An audit is formally requested by Customer's data protection authority; or **//** 顧客のデータ保護当局から、監査が正式に要求された場合

(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. **//** 強制力のある「データ保護法」により顧客に

直接的な監査権が与えられており、かつ顧客による監査の実施を、12 カ月間に 1 回のみとする場合（ただし、強制力のある「データ保護法」によってより頻度の多い監査が求められる場合はその限りではない）

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. **//** 他の管理者による監査 他の「管理者」は、第 5.1 条に記載するいずれかの場合が当該の他の「管理者」に当てはまる場合に限り、第 5.1 条に従って、SAP が処理する「個人データ」に関連する SAP の管理環境及びセキュリティ実務の監査を行うことができるものとする。かかる監査は、第 5.1 条に記載するとおり顧客を通じて及び顧客によって実施されなければならないが、当該の監査が、「データ保護法」に基づいて他の「管理者」により実施されなければならない場合はその限りではない。その「個人データ」が「本契約」に基づいて SAP により処理される複数の「管理者」が監査を求める場合、顧客は、あらゆる合理的な手段を用いて監査をまとめ、複数の監査を避けるものとする。

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. **//** 監査の範囲 顧客は、監査を行う場合には少なくとも 60 日前までに事前通知を行うものとするが、強制力のある「データ保護法」又はデータ保護当局によってより短期の通知が求められる場合はこの限りではない。監査の頻度及び範囲は、両当事者間で、合理的にかつ誠意をもって相互に合意されるものとする。顧客による監査は、最長で 3 営業日に限られるものとする。かかる制限を超えた場合、両当事者は最新の証明書又はその他の監査報告書を利用して、反復的な監査を避ける又は最小限にするものとする。顧客は、監査の結果を SAP に提供するものとする

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. **//** 監査の費用 顧客は、すべての監査の費用を負担するものとするが、かかる監査において SAP によるこの DPA の重大な違反が判明した場合は、SAP が監査の費用を自ら負担するものとする。監査により SAP がこの DPA 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。

6. SUBPROCESSORS // 処理外注先

6.1 **Permitted Use.** SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that: **//** 許可される使用 SAP は、以下を条件として、「個人データ」の処理業務を「処理外注先」に外注する全般的な権限を与えられる。

(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 又は SAP SE がその代理として、「処理外注先」による「個人データ」の処理に関連して、この DPA の条件と矛盾しない書面による（電子形式によるものを含む）契約書に基づいて「処理外注先」を従事させるものとする。SAP は、「処理外注先」による違反があった場合、「本契約」の条件に従って責任を負うものとする。

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and **//** SAP 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に関する実務を評価し、この DPA で求められる「個人データ」の保護の水準を提供する能力があることを立証するものとする。

(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. **//** 「本契約」の発効日において選定されている「処理外注先」の SAP のリストが SAP により公開されている、又は SAP が求めに応じてそれを顧客に提供すること。これには、「クラウドサービス」の提供のために SAP が使用する各「処理外注先」の名称、住所及び役割が記載されること。

6.2 **New Subprocessors.** SAP's use of Subprocessors is at its discretion, provided that: **//** 新規の処理外注先 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 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 は、「処理外注先」のリストに追加又は入れ替えを行おうとする場合、新規の「処理外注先」の名称、住所及び役割を記載して、事前に顧客に通告する（電子メールにより、又は SAP Support を通じて利用可能なサポートポータルへの掲出により）ものとする。

(b) Customer may object to such changes as set out in Section 6.3. **//** 顧客は、第 6.3 条に記載するとおり、かかる変更に異議を唱えることができる。

6.3 **Objections to New Subprocessors. //** 新規の処理外注先に対する異議

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor. **//** 新規の「処理外注先」による「個人データ」の処理について、「データ保護法」に基づいて異議を唱える正当な理由が顧客にある場合、顧客は、SAP への書面通知により、「本契約」（新規の「処理外注先」の使用が予定されている「クラウドサービス」に限る）を解除できるものとする。かかる解除は、顧客が決定する時点で発効するものとするが、新規の「処理外注先」に関して顧客に通告する SAP の顧客への通知の日付から 30 日後までとする。当該の 30 日間以内に顧客が解除しなかった場合、顧客は、新たな「処理外注先」を承認したものとみなされる。

(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. **//** 新規の「処理外注先」に関して顧客に通告する SAP の顧客への通知の日付から 30 日以内に、顧客は、異議の解消について協議するために、両当事者が誠意をもって会合することを要求できるものとする。かかる協議は、解除に向けた期間を延長するものとはならず、また新規の「処理外注先」を 30 日の期間後に使用する SAP の権利には影響を与えない。

(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. **//** 本第 6.3 条に基づく解除は、いずれの当事者による過失も伴わないとみなされるものとし、「本契約」の条件が適用されるものとする。

6.4 **Emergency Replacement.** SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement

Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly. **//** **緊急交代** SAP は、変更の理由が SAP の合理的な支配を超えたもので、セキュリティその他の緊急の事由により速やかな交代が必要な場合、事前の通知なくして「処理外注先」を交代させることができるものとする。この場合、SAP は、代替となる「処理外注先」について、その任命後可及的速やかに顧客に通知するものとする。第 6.3 条が適宜に適用される。

7. INTERNATIONAL PROCESSING // 海外での処理

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. **//** **海外での処理に関する条件** SAP は、「個人データ」の処理を、「処理外注先」を使用する場合を含め、この DPA に従って、「データ保護法」で許される、顧客が所在する国の国外で行うことができるものとする。

7.2 **Standard Contractual Clauses.** Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then: **//** **標準契約条項** (i) EEA 若しくはスイスに本拠を置く「管理者」の「個人データ」が、EEA、スイス、及び GDPR 第 45 条に基づく十分な水準のデータ保護が行われている国であると欧州連合により認められた国、組織若しくは地域外で処理される場合、又は (ii) 別の「管理者」の「個人データ」が海外で処理される場合であって、かかる海外での処理に当該「管理者」の国の法律に基づいて適切な手段が必要であり、「標準契約条項」を締結することによってかかる適切な手段が満たされる場合は、

(a) SAP and Customer enter into the Standard Contractual Clauses; **//** 顧客と SAP が、「標準契約条項」を締結する。

(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 **//** 顧客が、それぞれの関連する「処理外注先」と次のように「標準契約条項」を締結する。(i) 顧客が、SAP 若しくは SAP SE と「処理外注先」が締結した「標準契約条項」に、権利と義務の独立した保有者として参加する (「加盟モデル」) 又は、(ii) 「処理外注先」 (SAP により代表される) が、顧客と「標準契約条項」を締結する (「代理権モデル」)。「代理権モデル」は、第 6.1(c)条に基づいて提供された「処理外注先」のリスト又は顧客に対する通知を通じて「処理外注先」がその資格を有することを、SAP が明示的に確認した場合に、適用される。及び/又は

(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. **//** その「クラウドサービス」の利用が「本契約」に基づいて顧客により承認されている他の「管理者」も、上記第 7.2(a)条及び(b)条に従って、顧客と同様に SAP 及び/又は関連する「処理外注先」と「標準契約条項」を締結することができるものとする。その場合は、顧客が、当該の他の「管理者」に代わって「標準契約条項」を締結するものとする。

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. **//** 「本契約」に対する標準契約条項の関係　「本契約」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。疑義回避のために付記すれば、この DPA において第 5 条及び第 6 条に監査及び処理外注先に関する規則がさらに規定されている場合、かかる規定が、「標準契約条項」にも関連して適用される。

7.4 **Governing Law of the Standard Contractual Clauses.** The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated. **//** 標準契約条項の準拠法　「標準契約条項」には、関連する「管理者」が設立された国の法律が適用されるものとする。

8. DOCUMENTATION; RECORDS OF PROCESSING // 文書化、処理の記録

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. **//** 各当事者は、その文書化要件の遵守、とりわけ「データ保護法」に基づいて必要な場合に処理の記録を残しておくことに責任を負う。各当事者は、他方当事者が処理の記録を残しておくことに関連する義務に従うことができるよう、他方当事者が相手方から必要とする情報を他方当事者が合理的に要求する方法で（電子的システムを利用してなど）提供することも含め、合理的な範囲でその文書化要件において他方当事者を支援するものとする。

9. EU ACCESS // EU アクセス

9.1 **Optional Service.** EU Access is an optional service that may be offered by SAP. SAP shall provide the Cloud Service eligible for EU Access solely for production instances in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply. **//** オプションのサービス　「EU アクセス」は、SAP が提供する場合がある、オプションのサービスである。SAP は、本第 9 条に従って本稼動インスタンス用に限り、「EU アクセス」の対象である「クラウドサービス」を提供するものとする。「EU アクセス」が明示的に指摘されず、「注文書」においても合意されていない場合、本第 9 条は適用されないものとする。

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 アクセス　SAP は、欧州の「処理外注先」のみを使って、「クラウドサービス」内で「個人データ」へのアクセスを必要とするサポートを提供するとともに、SAP は、顧客により個別的に書面で明示的に承認されている、又は第 9.4 条に基づいて除外されている場合を除き、EEA 外又はスイス国外に「個人データ」をエクスポートしないものとする。

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. **//** データセンターの所在地　「本契約」の発効日において、「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 外又はスイス国外にある「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 内又はスイス国内の「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。

9.4 **Exclusions.** The following Personal Data is not subject to 9.2 and 9.3: **//** 除外規定 以下の「個人データ」は、第 9.2 条及び第 9.3 条の対象外とする。

(a) Contact details of the sender of a support ticket; and **//** 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. **//** 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。こ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。

10. DEFINITIONS // 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。

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. **//** 「管理者」とは、「個人データ」の処理の目的及び手段を、単独で又は他者と共同で決定する、自然人若しくは法人、公共団体、公的機関若しくはその他の組織をいい、この DPA においては、顧客が別の管理者に対する処理業者となる場合、顧客は SAP との関係において、この DPA に基づくそれぞれの管理者の権利及び義務を有する、追加の独立した「管理者」とみなされるものとする。

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. **//** 「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。

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). **//** 「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な権利及び自由並びにそのプライバシーの権利を保護する、該当する法律をいう（これには、顧客の代行としての SAP による「個人データ」の処理に関する両当事者の関係に関する限り、最低基準として GDPR が含まれ、これは「個人データ」が GDPR の対象であるかどうかを問わない）。

10.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law. **//** 「データ主体」とは、「データ保護法」で規定されている、特定された又は特定可能な自然人をいう。

10.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway. **//** 「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。

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

10.7 "Personal Data" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement). **//** **「個人データ」**とは、「データ保護法」で保護される「データ主体」に関する情報をいう。この DPA においては、次の個人データのみが含まれる。(i) 顧客又はその「認定ユーザー」により、「クラウドサービス」に入力された若しくは「クラウドサービス」から派生したもの、又は (ii) 「本契約」に基づくサポートの提供のために SAP 若しくはその「処理外注先」に供給された若しくはそれらによりアクセスされたもの。「個人データ」は、「顧客データ」(「本契約」で定義されている) のサブセットである。

10.8 "Personal Data Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects. **//** **「個人データ違反」**とは、確認された (1) 偶発的若しくは違法な、「個人データ」の破損、喪失、改変、不正な開示、若しくは第三者による「個人データ」へのアクセス、又は (2) 「個人データ」に関わる同様の付随事件で、いずれの場合も「データ保護法」に基づいて「管理者」が管轄のデータ保護当局又は「データ主体」に通知を行う必要があるものをいう。

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. **//** **「処理業者」**とは、「管理者」に代わって「個人データ」を処理する自然人若しくは法人、公共団体、公的機関若しくはその他の組織をいい、「管理者」の処理業者として直接的に、又は処理業者の処理外注先として間接的に、「管理者」に代わって「個人データ」を処理する場合がある。

10.10 "Standard Contractual Clauses or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses *current as of the effective date of the Agreement* are attached hereto as **Appendix 4. //** **「標準契約条項」**(「EU モデル条項」と呼ばれる場合もある) とは、欧州委員会により公開される「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)。 「本契約」の発効日において有効な「標準契約条項」が、この DPA の「付属書 4」として添付されている。

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. **//** **「処理外注先」**とは、「クラウドサービス」に関連して SAP、SAP SE 又は SAP SE の「関連会社」から委託を受けた、「SAP 関連会社」、SAP SE、「SAP SE 関連会社」及び第三者で、この DPA に従って「個人データ」を処理するものをいう。

11. Controlling Language // 支配言語

This DPA is executed in both the English and Japanese languages. in the event that there are differernt interpretations of the same provision or acutal contradictions between the two languages, the meanings of the English-language version shall prevail. **//** この DPA は、英語と日本語の両方の言語により締結される。同じ条項について 2 つの言語の間で解釈に相違が生じ、また実際に矛盾が生じた場合には、英語の意味が優先される。

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses
DPA （該当する場合は標準契約条項）の付属書 1

Data Exporter // データエクスポーター
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. **//** 「データエクスポーター」は、「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」に加入している顧客である。顧客が他の「管理者」にも「クラウドサービス」の利用を認める場合、それら他の「管理者」も「データエクスポーター」である。

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 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 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 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. **//** 「SAP SE 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 concerns the following categories of data: **//** 「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 Agreement (including 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：「本契約」（「注文書」を含む）に定めるとおり（ある場合）。

Processing Operations / Purposes // 処理業務/目的
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 the Agreement. **//** 「本契約」に従って行う、顧客の指示の実行

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures // DPA （該当する場合は標準契約条項）の付属書 2 – 技術的及び組織的対策

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"): **//** この「付属書 2」は技術的及び組織的対策（以下「本技術的及び組織的対策」）の 2 つのセットからなる。

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below. **//** 本技術的及び組織的対策（セット 1）（2018 年 4 月最終更新、その後修正なし）：以下に定義される本技術的及び組織的対策（セット 2）サービスを除いた全ての「クラウドサービス」に適用される。

- **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. **//** 本技術的及び組織的対策（セット 2）：本技術的及び組織的対策（セット 2）サービスにのみ適用される。2020 年 5 月 4 日付けで、本技術的及び組織的対策（セット 2）サービスとは、以下の「クラウドサービス」を意味する。SAP Analytics Cloud 及び SAP SuccessFactors and SAP Cloud Platform。SAP は、本技術的及び組織的対策（セット 2）サービスのリストから「クラウドサービス」をいつでも削除することができ、その場合当該「クラウドサービス」は本技術的及び組織的対策（セット 1）の適用を受けることとなる。

TOMs SET 1 // 本技術的及び組織的対策（セット 1）

Last Updated: April 2018 // 2018 年 4 月最終更新

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

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. **//** 以下のセクションでは、SAP の現行の技術的及び組織的対策を定める。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。個々の対策は、「個人データ」を保護するセキュリティレベルを損なわず同じ目的にかなう新たな対策に置き換えられる場合がある。

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. **// 物理的なアクセス制御** 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 the SAP Security Policy **//** SAP は、「SAP セキュリティポリシー」に基づく適切な手段を用いてそ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 protect 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。適切な機能性を保護するために、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 authorized personnel 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権限のある職員の名前及び時間を記録する。

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization. **// システムアクセス制御** 「クラウドサービス」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. Authorizations are managed via defined processes according to the SAP Security Policy **//** 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。権限は、「SAP セキュリティポリシー」に従った明確なプロセスで管理される。
- All personnel access SAP's systems with a unique identifier (user ID). **//** すべての職員は、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 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 では、要請された権限の変更が、「SAP セキュリティポリシー」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）。職員が退職する場合、そ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 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. **//** 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実施するために、セキュリティパッチ管理が導入されている。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. 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. **// データアクセス制御** 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 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. **//** 「個人データ」へのアクセスは、知る必要を基準として認められる。職員は、自身の職務を遂行するために必要な情報へのアクセス権を有する。SAP は、付与のプロセス及びアカウント（ユーザー ID）ごとに割り当てられた役割を文書化する、権限に関するコンセプトを用いる。すべての「顧客データ」は、「SAP セキュリティポリシー」に従って保護される。
- 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. **//** 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。「個人データ」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 software that has not been approved by SAP. **//** SAP では、SAP が承認していない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. 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). **// データ伝送制御** 「本契約」に従って「クラウドサービス」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提供するために 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）。

Measures: **//** 対策

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy. **//** SAP の社内ネットワーク上で転送される「個人データ」は、「SAP セキュリティポリシー」に従って保護される。
- 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. 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. **// データ入力制御** 「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 personnel to access Personal Data as required in the course of their duty. **//** SAP は、権限を有する職員のみに、その職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 the Cloud Service to the extent technically possible. **//** SAP は、技術的に可能な範囲で、「クラウドサービス」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. 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. **// ジョブ制御** 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「本契約」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 monitor 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監視するための、管理手段及び手順を用いる。

- 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 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。

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss. **// 可用性制御** 「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 regular backup processes to provide restoration of business-critical systems as and when necessary. **//** SAP は、必要に応じて業務上不可欠なシステムの復元を行うための、定期的なバックアッププロセスを採用する。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers. **//** SAP は、「データセンター」への電力供給を確保するため、無中断の電源（たとえば、UPS、バッテリー、発電機など）を使用する。
- 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 は、業務上不可欠なプロセスに関する事業非常事態計画を定めており、「ドキュメンテーション」に詳細が記載されている、又は関連する「クラウドサービス」の「注文書」に組み込まれているとおり、業務上不可欠な「サービス」に対して災害復旧戦略を提供する場合がある。
- 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. Personal Data collected for different purposes can be processed separately. **// データ分離制御** 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。

- Customer (including its Controllers) has access only to its own data. **//** 顧客（その「管理者」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 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、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. Personal Data will remain intact, complete and current during processing activities. **//** **データ完全性制御** 「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. 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

TOMs SET 2 // 本技術的及び組織的対策（セット 2）

(*applies to TOMs Set 2 Services defined above*) // （上記にて定義される本技術的及び組織的対策(その2)サービスに適用される）

Last Updated: May 4 2020 // 2020 年 5 月 4 日最終更新

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

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. **//** 以下のセクションでは、SAP の現行の技術的及び組織的対策を定める。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。個々の対策は、「個人データ」を保護するセキュリティレベルを損なわず同じ目的にかなう新たな対策に置き換えられる場合がある。

1.1 Physical Access Control.

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy **//** SAP は、「SAP セキュリティポリシー」に基づく適切な手段を用いてそ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 protect 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。適切な機能性を保護するために、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 authorized personnel 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権限のある職員の名前及び時間を記録する。

1.2 System Access Control.

- 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 **//** 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。権限は、「SAP セキュリティポリシー」に従った明確なプロセスで管理される。
- All personnel access SAP's systems with a unique identifier (user ID). **//** すべての職員は、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 policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked. **//** SAP は、承認なしにいかなる権利も付与されず、職員が退職する場合、そのアクセス権は取り消されることを規定しようとするポリシーを有している。
- 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 process to deploy relevant security updates on a regular and periodic basis. Full remote access to SAP's corporate network and critical infrastructure is protected by authentication. **//** 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のためのセキュリティパッチ管理手順。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、認証によって保護されている。

1.3 Data Access Control.

- 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 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. **//** 「個人データ」へのアクセスは、知る必要を基準として認められる。職員は、自身の職務を遂行するために必要な情報へのアクセス権を有する。SAP は、付与のプロセス及びアカウント（ユーザー ID）ごとに割り当てられた役割を文書化する、権限に関するコンセプトを用いる。すべての「顧客データ」は、「SAP セキュリティポリシー」に従って保護される。
- 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. **//** 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。「個人データ」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/又は侵入テストを実施している。
- Processes and policies to detect the installation of unapproved software on production systems. **//** 未承認のソフトウェアの本稼働システムへのインストールを検知する手順及びポリシー。
- 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.

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy. **//** SAP の社内ネットワーク上で転送される「個人データ」は、「SAP セキュリティポリシー」に従って保護される。
- 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.

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty. **//** SAP は、権限を有する職員のみに、その職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 in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible. **//** SAP は、ほとんどの場合に、技術的に可能な範囲で、「クラウドサービス」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.

- SAP uses controls and processes to monitor 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監視するための、管理手段及び手順を用いる。

- 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 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。

1.7 Availability Control.

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary. **//** SAP は、必要に応じて業務上不可欠なシステムの復元を行うための、定期的なバックアッププロセスを採用する。
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers. **//** SAP は、「データセンター」への電力供給を確保するため、無中断の電源（たとえば、UPS、バッテリー、発電機など）を使用する。
- 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 は、業務上不可欠なプロセスに関する事業非常事態計画を定めており、「ドキュメンテーション」に詳細が記載されている、又は関連する「クラウドサービス」の「注文書」に組み込まれているとおり、業務上不可欠な「サービス」に対して災害復旧戦略を提供する場合がある。
- 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.

- 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。

- Customer (including its Controllers) has access only to its own data. **//** 顧客（その「管理者」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 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、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.

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. 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 and/or regular external audits to prove security measures. **//** 外部及び内部の侵入テスト及び/又はセキュリティ対策を証明する定期的な外部監査

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses
DPA （該当する場合は標準契約条項）の付属書 3

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only. **//** 以下の表には、GDPR の関連する条項と対応する DPA の項目を、専ら説明目的で記載している。

Article of GDPF	**Section of DPA**	**Click on link to see Section**
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures
28(2), 28(3) (d) and 28 (4)	6	Subprocessors
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application Structure
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures
28(3) (e)	3.4	Cooperation
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion.
28(3) (h)	5	Certifications and Audits
28 (4)	6	Subprocessor
30	8	Documentation; Records of processing.
46(2) (c)	7.2	Standard Contractual Clauses.

Appendix 4
付属書 4

[The Standard Contractual Clauses set out in this Appendix 4 are current as at 31 March 2018, and the Japanese translation is provided as a matter of convenience only. These Standard Contractual Clauses are automatically subject to updates by the European Commission and as subsequently published by the European Commission, Customer should always access the URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 for updated versions of the Standard Contractual Clauses. Customer's local language may not be supported at the European Commission, or at URL, and it will be Customer's responsibility to ensure that it is aware of the current version/s of the Standard Contractual Clauses and manages any necessary translations of any updates of those Standard Contractual Clauses]

この「付属書 4」で規定される「標準契約条項」は、2018 年 5 月 31 日時点において有効であり、日本語の対訳は、便宜のための参考訳としてのみ提供される。この「標準契約条項」は、欧州委員会により、自動的に更新される可能性があり、それに応じて欧州委員会により公表される。欧州委員会又は以下の URL においてでは、顧客の現地の言語についてをサポートしていない場合がある。顧客は、かかる「標準契約条項」の更新版に常時、以下の URL を通してアクセスするものとし（https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087）、顧客の責任において「標準契約条項」の最新版を把握し、かかる「標準契約条項」のすべての更新に対して必要とされる翻訳を行うものとする。

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]
標準契約条項（処理業者）[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection **//** 十分なレベルの「データ」保護を保証していない第三国で登記された処理業者に対する個人データの転送に関する、指令 95/46/EC 第 26(2) 条（又は、2018 年 5 月 25 日以降については、規則 2016/79 の第 44 条以下）について、

Customer also on behalf of the other Controllers // 顧客（また他の「管理者」に代わって）
(in the Clauses hereinafter referred to as the '**data exporter**') **//** （以下、「条項」において「**データエクスポーター**」という）

and **//** 及び

SAP // SAP
(in the Clauses hereinafter referred to as the '**data importer**') **//** （以下、「条項」において「**データインポーター**」という）は

each a 'party'; together 'the parties', **//** （それぞれを「当事者」、まとめて「両当事者」という）

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)
[1] 2010 年 2 月 5 日の欧州委員会の決定に基づく（2010/87/EU）

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. **//** 「付属書 1」に記載された個人データをデータエクスポーターからデータインポーターに転送する場合の、個人のプライバシー及び基本的な権利と自由の保護に関する十分な予防措置を提示するために、以下の「契約条項」（「条項」）に合意した。

Clause 1 **//** *第 1 条*

Definitions // 定義

For the purposes of the Clauses: **//** 「条項」において

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; **//** 「個人データ」、「特別カテゴリーのデータ」、「処理」、「管理者」、「処理者」、「データ主体」、及び「監督機関」は、個人データ処理に係る個人の保護及び当該データの自由な移動に関する、欧州議会及び理事会の指令 95/46/EC （1995 年 10 月 24 日）における意味と同じ意味を有するものとする。

(b) 'the data exporter' means the controller who transfers the personal data; **//** 「データエクスポーター」とは、個人データを転送する管理者をいう。

(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; **//** 「データインポーター」とは、処理者をいい、データエクスポーターの指示及び「条項」の条件に従って転送された後に、データエクスポーターに代わって処理する対象の個人データをデータエクスポーターから受領することに同意する。またデータインポーターは、指令 95/46/EC 第 25(1) 条の意味する範囲で十分な保護を保証している第三国のシステムには従わないものとする。

(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; **//** 「処理外注先」とは、データインポーター、又はデータインポーターのその他処理外注先から委託を受けた処理業者をいい、データエクスポーターの指示、「条項」の条件、及び書面による下請契約に従って転送された後に、データエクスポーターに代わって実行される処理作業に目的を限定した個人データを、データインポーター、又はデータインポーターのその他処理外注先から受領することに同意する。

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; **//** 「適用データ保護法」とは、データエクスポーターが登記された「加盟国」のデータ管理者に適用される、個人の権利及び自由、とりわけ個人データの処理に関するプライバシーの権利を保護する法律をいう。

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. **//** 「技術的及び組織的なセキュリティー対策」とは、個人データを、偶発的若しくは非合法的な破壊又は偶発的な喪失、変更、不正な開示若しくはアクセス（とりわけ、処理がネットワークを介したデータの転送にかかわる場合）、及びその他すべての非合法的な形の処理から保護することを目的とした対策をいう。

Clause 2 **//** *第 2 条*

Details of the transfer // 転送に関する詳細

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. **//** 転送の詳細、及びとりわけ該当する場合、特別カテゴリーの個人データについては、「付属書 1」（「条項」の不可欠の部分を成す）に明記されている。

Clause 3 **//** *第 3 条*

Third-party beneficiary clause // 第三受益者に関する条項

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. **//** データ主体は、第三受益者として、本条及び以下の条項をデータエクスポーターに強制することができる。第 4 条 (b) から (i)、第 5 条 (a) から (e) 及び (g) から (j)、第 6 条 (1) 及び (2)、第 7 条、第 8(2) 条、並びに第 9 条から第 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. **//** データエクスポーターが、事実上消滅したか、又は法律上存在しなくなった場合は、データ主体は、第三受益者として、本条及び以下の条項をデータインポーターに強制することができる。第 5 条 (a) から (e) 及び (g)、第 6 条、第 7 条、第 8(2) 条、並びに第 9 条から第 12 条。ただし、承継法人が、契約又は法律の運用によりデータエクスポーターの法律上の義務の全体を引き継ぎ、その結果として、承継法人がデータエクスポーターの権利及び義務を引き受ける場合を除く。その場合は、データ主体は、当該法人に上記条項を強制することができる。

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. **//** データエクスポーター及びデータインポーターの両方が、事実上消滅したか、法律上存在しなくなったか、支払い不能に陥った場合は、データ主体は、第三受益者として、本条及び以下の条項を処理外注先に強制することができる。第 5 条 (a) から (e) 及び (g)、第 6 条、第 7

条、第 8(2) 条、並びに第 9 条から第 12 条。ただし、承継法人が、契約又は法律の運用によりデータエクスポーターの法律上の義務の全体を引き継ぎ、その結果として、承継法人がデータエクスポーターの権利及び義務を引き受ける場合を除く。その場合は、データ主体は、当該法人に上記条項を強制することができる。処理外注先のかかる第三者の責任は、「条項」に基づく自らの処理業務に限定される。

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. **//** 両当事者は、データ主体がそれを明示的に希望しており、国内法で許可されている場合は、組合又はその他組織体がデータ主体を代表することに反対しないものとする。

Clause 4 **//** *第 4 条*

Obligations of the data exporter // データエクスポーターの義務

The data exporter agrees and warrants: **//** データエクスポーターは、以下のことに同意し、保証する。

(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; **//** 個人データの処理（その転送を含む）は、これまでも今後も引き続き、適用されるデータ保護法の関連条項に従って実行され（及び、該当する場合は、データエクスポーターが登記された「加盟国」の関連当局に通知が行われた）、当該国の関連条項に違反していないこと。

(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; **//** データエクスポーターの代理としてのみ、適用されるデータ保護法及び「条項」に従って転送された個人データを処理することについて、データインポーターに対してすでに指示したこと、及び個人データ処理サービスの期間を通して指示すること。

(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; **//** データインポーターが、この契約の「付属書 2」に記載する技術的及び組織的なセキュリティ対策に関して十分に保証すること。

(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; **//** 適用されるデータ保護法の要件を評価した後、セキュリティー対策が、偶発的若しくは非合法的な破壊又は偶発的な喪失、変更、不正な開示若しくはアクセス（とりわけ、処理がネットワークを介したデータの転送にかかわる場合）、及びその他すべての非合法的な形の処理から個人データを保護するために適切であること、並びにこれらの対策が、その水準と導入費用を考慮に入れ、処理によってさらされるリスク及び保護対象のデータの性質に対して適切なセキュリティーレベルを満たしていること。

(e) that it will ensure compliance with the security measures; // セキュリティー対策が遵守されるよう万全を期すこと。

(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; // 転送が特別なカテゴリーのデータに関わる場合は、データ主体に対して、指令 95/46/EC の意味する範囲で十分な保護が講じられていない第三国にそのデータが転送される可能性があることを、すでに通知したか、転送の前に又は転送後可能な限り速やかに通知するものとする。

(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; // データエクスポーターが転送の継続、又は停止の解除を決定した場合、第 5(b) 条及び第 8(3) 条に従って、データインポーター又は処理外注先から受領した通知を、データ保護の監督機関に転送する。

(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; // 要請に応じて、データ主体に対して、「付属書 2」を除く「条項」、及びセキュリティー対策の概要書のコピー、並びに「条項」に従って締結するべき処理外注サービスに関する契約書のコピーを提供する。ただし、「条項」又は契約書に商用情報が含まれている場合を除く。その場合、データエクスポーターは、かかる商用情報を削除することができる。

(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 // 処理を外注する場合、処理業務は、「条項」に基づき個人データ及びデータ主体の権利に対してデータインポーターと少なくとも同じレベルの保護を提供する処理外注先により、第 11 条に従って実行されること。

(j) that it will ensure compliance with Clause 4(a) to (i). // 第 4 条 (a) から (i) を確実に遵守すること。

Clause 5 // 第 5 条

Obligations of the data importer // データインポーターの義務

The data importer agrees and warrants: // データインポーターは、以下のことに同意し、保証する。

(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; // データエクスポーターの代理としてのみ、その指示及び「条項」を遵守して個人データを処理すること。理由に関わらずかかる遵守が不可能な場合は、データインポーターは、遵守できない旨を速やかにデータエクスポー

ターに通知することに同意する。その場合、データエクスポーターは、データの転送を中止するか、及び/又は契約を解除することができる。

(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; **//** データインポーターに適用される法律により、データエクスポーターから受領する指示、及び契約に基づくその義務の履行が妨げられると信じる理由はないこと。またかかる法律に変更があり、「条項」に定める保証及び義務に相当な悪影響が及ぶことが考えられる場合は、知るところとなり次第速やかに当該変更をデータエクスポーターに通知するものとする。その場合、データエクスポーターは、「データ」の転送を中止するか、及び/又は契約を解除することができる。

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred; **//** 転送された個人データを処理する前に、「付属書 2」に記載された技術的及び組織的なセキュリティ対策を導入したこと。

(d) that it will promptly notify the data exporter about: **//** 以下について、速やかにデータエクスポーターに通知すること。

(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; **//** 法執行機関による、法的に拘束力のある個人データ開示請求。ただし、法執行機関の取調べの秘密を保護する刑法に基づく禁止など、禁止された場合を除く。

(ii) any accidental or unauthorised access; and **//** 偶発的又は不正なアクセス

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so; **//** データ主体から直接、要求を受領しても、別途応答する権限を付与されている場合を除いて、その要求に応答しないこと。

(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; **//** 転送の対象である個人データの処理に関するデータエクスポーターのすべての問い合わせについて、速やかにかつ適切に対応し、また転送されたデータの処理に関して監督機関の助言を守ること。

(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; **//** データエクスポーターの要請があれば、そのデータ処理施設を、「条項」の対象である処理業務の監査に委ねるものとする。この監査は、データエクスポーター、又は監督機関に従い該当する場合は、独立的な成員で構成され、必要な専門資格を有し守秘義務を負う、データエクスポーターが選択する調査機関によって実施される。

(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; **//** 要請に応じて、データ主体に対して、「条項」、又は処理外注に関する既存の契約書のコピーを提供する。ただし、「条項」又は契約書に商用情報が含まれている場合を除く。その場合、データインポーターは、かかる商用情報を削除することができる。また、「付属書 2」を除く。「付属書 2」は、データ主体がセキュリティー対策概要書のコピーをデータエクスポーターから入手できない場合、同概要書で置き換えるものとする。

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent; **//** 処理を外注する場合は、あらかじめデータエクスポーターに通知し、その書面による同意を事前に取得する。

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11; **//** 処理外注先による処理サービスは、第 11 条に従って実施される。

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter. **//** 「条項」に基づき締結した処理外注先の契約書のコピーを、速やかにデータエクスポーターに送付する。

Clause 6 **//** *第 6 条*

Liability // 責任

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered. **//** 両当事者は、いずれかの当事者又は処理外注先による第 3 条又は第 11 条で言及する義務の違反に起因する損害を被ったデータ主体は、被った損害についてデータエクスポータから補償を受ける権利を有することに合意する。

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. **//** データインポーター又はその処理外注先による第 3 条又は第 11 条で言及するそれらの義務の違反に起因する場合に、データエクスポーターが事実上消滅したか、法律上存在しなくなったか、又は支払い不能に陥ったために、データ主体が第 1 項に従ってデータエクスポーターに対して補償を請求することができない場合は、データインポーターがデータエクスポーターであるかのように、データ主体がデータインポーターに請求を行うことができることに、データインポーターは同意するものとする。ただし、承継法人が、契約又は法律の運用によりデータエクスポーターの法律上の義務の全体を引き継いだ場合を除く。その場合、データ主体は、当該法人に自身の権利を強制することができる。

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities. // データインポーターが、自身の責任を逃れるために、処理外注先がその義務に違反したことを理由とすることは認められない。

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. // 処理外注先による第 3 条又は第 11 条で言及するその義務の違反に起因する場合に、データエクスポーターとデータインポーターの両方が事実上消滅したか、法律上存在しなくなったか、又は支払い不能に陥ったために、データ主体が第 1 項及び第 2 項で言及されるようにデータエクスポーター又はデータインポーターに対して請求を提起することができない場合は、処理外注先がデータエクスポーター又はデータインポーターであるかのように、「条項」に基づく処理外注先の処理業務に関してデータ主体が処理外注先に請求を行うことができることに、処理外注先は同意するものとする。ただし、承継法人が、契約又は法律の運用によりデータエクスポーター又はデータインポーターの法律上の義務の全体を引き継いだ場合を除く。その場合は、データ主体は、当該法人に自身の権利を強制することができる。処理外注先の責任は、「条項」に基づく自身の処理業務に限定される。

Clause 7 // 第 7 条

Mediation and jurisdiction // 調停及び管轄権

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: // データインポーターは、データ主体が自身に対して第三受益者の権利を援用するか、及び/又は「条項」に基づいて補償を請求する場合は、データ主体の以下の決定を受け入れることに同意するものとする。

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; // 独立的な個人、又は該当する場合は監督機関による調停に、紛争を委ねる。

(b) to refer the dispute to the courts in the Member State in which the data exporter is established. // データエクスポーターが登記された「加盟国」の裁判所に、紛争を委ねる。

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. // 両当事者は、データ主体が行った選択は、国内法又は国際法のその他の条項に従って救済を求めるデータ主体の実体的又は手続上の権利を損なうものではないことに合意する。

Clause 8 **//** *第 8 条*

Cooperation with supervisory authorities // 監督機関との協力

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. **//** データクスポーターは、その要請があったか、又は適用されるデータ保護法に基づいて提出が必要な場合は、この契約書のコピーを監督機関に提出することに同意する。

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. **//** 両当事者は、監督機関がデータインポーター及び処理外注先の監査を実施する権利を有することに合意する。この監査は、適用されるデータ保護法に基づくデータエクスポーターの監査と同じ範囲で行われ、それに適用される条件と同じ条件に従うものとする。

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). **//** データインポーターは、自身又は処理外注先に適用される法律で、第 2 項に基づくデータインポーター又は処理外注先に対する監査の実施を妨げるものがあれば、速やかにデータエクスポーターに通知するものとする。かかる場合は、データエクスポーターは、前記第 5(b) 条の措置を取ることができる。

Clause 9 **//** *第 9 条*

Governing law // 準拠法

The Clauses shall be governed by the law of the Member State in which the data exporter is established. **//** 「条項」には、データエクスポーターが登記された「加盟国」の法律が適用される。

Clause 10 **//** *第 10 条*

Variation of the contract // 契約の変更

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. **//** 両当事者は、「条項」を変更又は修正しないことを約束する。このことは、必要な場合に「条項」と相反しないことを条件として、両当事者が事業関連の問題に条項を追加することを妨げない。

Clause 11 **//** *第 11 条*

Sub-processing // 処理の外注

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. **//** データインポーターは、データエクスポーターの書面による同意を事前に得ることなく、「条項」に基づきデータエクスポーターに代わって自身が実施するいかなる処理業務も外注してはならない。データエクスポーターの同意により、データインポーターが「条項」に基づく自身の義務を外注する場合は、データインポーターは、必ずその前提として、「条項」に基づきデータインポーターに課される義務と同じ義務を処理外注先に課す書面による契約を処理外注先と結ぶものとする。処理外注先がかかる書面による契約に基づくデータ保護義務を履行できなかった場合、データインポーターは、かかる契約に基づく処理外注先の義務の履行について、引き続き完全な責任をデータエクスポーターに対して負うものとする。

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. **//** データインポーターと処理外注先の間で結ばれる事前の契約書においても、以下の場合に関して第 3 条に定める第三受益者の条項を定めるものとする。データエクスポーターとデータインポーターの両方が事実上消滅したか、法律上存在しなくなったか、又は支払い不能に陥ったために、データ主体が、第 6 条第 1 項で言及されるようにデータエクスポーター又はデータインポーターに対して補償を請求することができず、契約又は法律の運用によりデータエクスポーター又はデータインポーターの法律上の義務の全体を引き継ぐ承継法人がない場合。処理外注先のかかる第三者の責任は、「条項」に基づく自らの処理業務に限定される。

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 項で言及される契約に含まれた処理外注におけるデータ保護の側面に関する条項には、データエクスポーターが登記された「加盟国」の法律が適用される。

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. **//** データエクスポーターは、「条項」に基づいて締結され、第 5(j) 条に従ってデータインポーターから通知を受けた処理外注契約書のリストを保持し、少なくとも 1 年に 1 回更新するものとする。かかるリストは、データエクスポーターのデータ保護監督機関に提供できるものとする。

Clause 12 **//** *第 12 条*

Obligation after the termination of personal data-processing services // 個人データ処理サービスの終了後の義務

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore. **//** データ処理サービスの提供が終了すれば、データインポーター及び処理外注先は、データエクスポーターの選択により、転送されたすべての個人データ及びそのコピーをデータエクスポーターに返却するか、又はすべての個人データを破棄し、その旨をデータエクスポーターに対して確認することに、両当事者は合意する。ただし、データインポーターに課される法律により、転送された個人データのすべて又は一部を返却又は破棄することが禁じられる場合は、この限りでない。その場合は、データインポーターは、転送された個人データの機密を約束すること、及び以降は転送された個人データを自発的に処理しないことを保証する。

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. **//** データインポーター及び処理外注先は、データエクスポーター及び/又は監督機関の要請があれば、第 1 項で言及する措置について、データ処理施設を監査に委ねることを保証する。