データ処理補遺条項（従前の SaaS 補遺条項）

本データ処理補遺条項（以下「**本DPA**」という）は、特定のSaaSソフトウェア ライセンス、保守サービスおよびコンサルティング サービス、またはこれらのいずれか（以下、本DPAにおいて「**本サービス**」という）の購入に関するプロバイダと顧客との間のソフトウェア契約およびサービス契約、またはこれらのいずれか（以下「**本契約**」という）に組み込まれ、プロバイダと顧客との間の書面（電子的形態を含む）による契約の一部を構成する。頭文字が大文字で表記された用語のうち、本DPAにおいて定義されていないものは、いずれも本契約で定義された意味を有するものとする。

1. 定義。頭文字が大文字で表記された用語のうち、文脈または本契約において定義されていないものは、以下に規定する意味を持つものとする。

a) 「***データ管理者***」とは、単独または他者と共同で、個人データの処理の目的および手段を決定する自然人、法人、公的当局、公的機関またはその他の主体を意味する。

b) 「***データ保護法***」とは、本契約に基づく顧客の個人データの処理に適用されるすべての法令を意味する。これには、場合に応じて以下が含まれる。（i）カリフォルニア州プライバシー権法（California Privacy Rights Act）により改正されたカリフォルニア州消費者プライバシー法（California Consumer Privacy Act）、および同法に基づき公布された、拘束力を有する一切の規則（以下「**CCPA**」という）、（ii）一般データ保護規則（General Data Protection Regulation。規則（EU）2016/679）（以下「**EU GDPR**」または「**GDPR**」という）、（iii）データ保護に関するスイス連邦法（Swiss Federal Act on Data Protection）（以下「**FADP**」という）、（iv）2018 年 EU（離脱）法（European Union (Withdrawal) Act 2018）の第 3 条により、イングランドおよびウェールズの法律の一部を構成する EU GDPR（以下「**英国 GDPR**」という）、ならびに（v）2018 年英国データ保護法（UK Data Protection Act 2018）。なお、いずれの場合も、随時更新、改定または差し替えられた場合は、更新後、改定後または差替え後の内容による。

c) 「***データ主体***」とは、顧客の個人データに関連する、識別された自然人または識別可能な自然人を意味する。

d) 「***個人データ***」とは、識別された自然人もしくは識別可能な自然人に関する情報、またはデータ保護法で定義された「個人データ」、「個人情報」、「個人識別が可能な情報」、もしくはこれらに類する用語に該当する情報を意味する。

e) 「***個人データの侵害***」とは、プロバイダが処理する顧客の個人データに生じた偶発的または違法な破壊、紛失、改変、不当開示または無権限の第三者によるアクセスであり、いずれの場合に関しても、データ保護法に基づき、所管のデータ保護当局またはデータ主体への通知が管理者に義務付けられているものを意味する。

f) 「***処理***」とは、収集、記録、整理、構造化、保存、改変もしくは変更、検索、参照、使用、送信による開示、頒布もしくはその他の方法による提供、配列もしくは組合せ、制限、削除または破壊等、個人データに対して実行されるあらゆる操作（自動化された手法によるか否かを問わない）を意味する。

g) 「***処理者***」とは、管理者に代わり個人データを処理する自然人、法人、公的当局、公的機関またはその他の主体を意味する。

h) 「***標準契約条項***」または「**EU SCC**」とは、欧州委員会が決定 2021/914 において承認した標準契約条項を意味する。

i) 「***復処理者***」とは、プロバイダの関連会社、または本サービスの一部もしくは全部の提供を行わせるためにプロバイダ（またはプロバイダの関連会社）が委託している第三者であり、本 DPA に従い顧客の個人データの処理を行う者を意味する。

2. 顧客の個人データの処理

プロバイダは、管理者である顧客に代わり行為する処理者として（または、処理者である顧客に代わる復処理者として）、本契約に基づき顧客の個人データを処理することができる。プロバイダは、（i）本DPAおよび本契約、ならびに（ii）顧客の書面による指示に基づくプロバイダの顧客に対する義務を履行すること、または（iii）適用法に基づくプロバイダの義務を遵守することのみを目的として、データ保護法に基づく通知義務に従い、個人データを処理することを約束する。処理の主題、処理の期間、性質および目的、ならびに顧客の個人データの種類およびデータ主体に関する詳細は、本契約に規定の通りである。また、本契約に規定がない場合は、本DPAの別紙1に規定された通りとする。顧客およびプロバイダは、本サービスに関連して処理される個人データに適用されるデータ保護法に基づく各自の義務を遵守することに同意する。顧客は、プロバイダに個人データを開示、送信またはその他の方法で提供する以前は、顧客の個人データの処理に関するデータ保護法を遵守する責任を単独で負う。プロバイダは、顧客の指示がデータ保護法に違反するものと思料する場合は、直ちに顧客に通知するものとする。

3. 処理のセキュリティ

a) **一般的なセキュリティ ポリシー。**プロバイダは、本契約で参照され、https://www.oneidentity.com/legal/security.aspx（集合的に「***セキュリティ サイト***」という）でさらに詳述されているプロバイダのセキュリティ対策に従い、顧客の個人データの性質に即して、技術的および組織的な措置、手続および慣行（顧客の個人データのセキュリティ、秘密性、完全性および可用性を保護すること、ならびに顧客の個人データを個人データ侵害から保護することを目的に設計されたもの）を実施し、これを維持する。これには、以下が含まれる。

- 情報セキュリティ ポリシー、
- 技術的および組織的な対策の表明
- データ侵害対応ポリシー、および
- プライバシー ポリシー

プロバイダは、提供される保護の全体的レベルが著しく低下しない限り、セキュリティ サイトを修正することができる。

b) **秘密保持。**プロバイダは、本契約に規定されたプロバイダの秘密保持義務に従い、顧客の個人データを保護する。プロバイダは、顧客の個人データの処理を行う人員が、書面による秘密保持契約を締結済みであることを確認する。プロバ

イダは、上記の秘密保持義務が、上記人員の雇用終了後も存続することを確認するものとする。プロバイダは、顧客の個人データへのアクセス権を有する個人に対して、データ セキュリティおよびデータ プライバシーに関する要求事項および諸原則に関する研修を定期的に行う。

4. データ主体の要請。

プロバイダは、顧客の要請に応じて、顧客がデータ保護法に基づく義務（データ保護法に基づく権利行使を求める個人の要請に応じるという義務）を遵守することを支援するため、商業上合理的な措置を講じる。ただし、顧客が単独で（本サービスを使用する場合を含む）上記要請を充足することが合理的に不可能な場合に限る。本書に基づき処理されている個人データに関して、プロバイダがデータ主体から要請を受領した場合、プロバイダは、（データ主体が顧客を特定するための情報を提供した場合は）当該要請を顧客に転送するよう当該データ主体に指示する。

5. 監査権。

a) **プロバイダの記録全般。**プロバイダは、データ保護法に従い、自らが行う処理に関する記録を作成する。また、顧客による書面での要請に応じて、本DPAおよび適用されるデータ保護法に基づくプロバイダの義務が遵守されていることを証明するために合理的に必要とされる記録を顧客に提供する。

b) **第三者のコンプライアンス プログラム。**プロバイダは、顧客による書面での要請に応じて、プロバイダの第三者による監査および認証プログラム（存在する場合）について説明を行い、その監査報告書（各報告書を「**監査報告書**」という）のコピーを顧客に提供する（ただし、本契約に規定された秘密保持義務を前提とする）。顧客は、必要に応じて、関係する政府当局と監査報告書のコピーを共有することができる。

c) **顧客による監査。**顧客は、相互に合意された計画（次のパラメータに適合するもの）に従い、自らの費用負担で監査を実施することができる（以下「**監査**」という）。顧客は、（1）プロバイダが監査報告書を提供しても、プロバイダによる本DPAまたはデータ保護法の遵守状況を検証するための十分な情報が提供されない場合、または（2）顧客が政府当局による監査に対応するために必要な場合、または（3）個人データ侵害に関連する場合に、監査権を行使することができる。

各監査は、以下を満たすものでなければならない。（1）プロバイダと事前に秘密保持契約を締結した独立した第三者が実施すること。（2）顧客がプロバイダによる本DPAの遵守状況および当事者らによるデータ保護法の遵守状況を評価するために合理的に必要とされる事項に範囲を限定すること。（3）相互に合意された日時に、かつプロバイダの通常の営業時間内にのみ実施すること。（4）年に1回を上限とすること（データ保護法に基づき要求される場合、または個人データ侵害に関連して実施する場合を除く）。（5）プロバイダが管理する施設のみを対象とすること。（6）調査対象を顧客の個人データのみに制限すること。（7）データ保護法で許容される最大限の範囲で、一切の結果を秘密情報として扱うこと。

6. 復処理者と国際的移転。

a) **復処理者の使用。**顧客は、プロバイダが本サービスのプロビジョニングに関して復処理者を使用することを原則的に許可する。プロバイダは、本DPAの規定および本書に規定された顧客とプロバイダとの間の指示事項に従い、復処理者と適切な書面契約を締結するものとする。プロバイダは、プロバイダが使用する復処理者が生じさせた本DPA違反に対して責任を負う。

b) **復処理者のリスト。**プロバイダは、https://support.oneidentity.com/subprocessorで登録を行うことで顧客に閲覧可能となる、ソフトウェア製品ごとの復処理者のリスト（復処理者の機能および所在地を含む）を管理する。プロバイダは、新たな復処理者に個人データへのアクセス権限を付与する30日前までに、復処理者のリストを更新し、登録時に提供された電子メール アドレスに宛て、顧客への通知を行う。

c) **新たな復処理者への異議。**顧客は、新たな復処理者を承認しない場合、通知期間の終了前に書面による解除通知（不承認の理由の説明を記載したもの）を提供することにより、該当するSaaSソフトウェアのサブスクリプションを解除することができる。

d) **国際的移転。**欧州および英国またはそのいずれか一方の個人データを、個人データに対する十分な保護を提供していない第三国に所在する復処理者に移転する場合について、プロバイダおよび当該復処理者は、欧州および英国のデータ保護法に従って当該個人データの移転に適切な保護措置を提供するため、EU SCCを締結している。

7. 個人データ侵害の通知。

セキュリティ サイトに規定された義務に加えて、プロバイダは、個人データ侵害を認識した後、速やかに顧客に通知を行い、顧客による義務（データ保護法で要求される、個人データ侵害を報告する義務）の充足を支援するために合理的情報を提供する。プロバイダは、上記情報が入手可能となった時点で、段階的にこれを提供することができる。プロバイダは、個人データ侵害の原因を特定するために誠実に努力すること、また、当該個人データ侵害の原因を是正するために必要かつ合理的であるとプロバイダが判断する措置を講じることに同意する。

8. 顧客の個人データの削除。

顧客が、本契約の解除または満了後、本サービスが終了する30日前までにプロバイダに通知を行った場合を除き、プロバイダはプロバイダのシステムから顧客の個人データをすべて削除する。プロバイダは、業界標準の安全な削除方法に従い削除を実行する。上記にかかわらず、プロバイダは、（i）データ保護法の要求、または（ii）プロバイダの標準的なバックアップ ポリシーまたは記録保持ポリシーに従い、顧客の個人データを保持することができる。ただし、いずれの場合も、プロバイダが、（1）保持する顧客の個人データに関して秘密を保持するとともに本DPAの適用条項を遵守すること、（2）保持する顧客の個人データのさらなる処理（適用されるデータ保護法に規定された目的のため、同法に規定された期間にわたり行うものを除く）を行わないことを条件とする。

9. データ保護影響評価。

プロバイダは、データ保護法に基づく顧客の義務（顧客による本サービスの使用に関し、データ保護影響評価またはこれに類似するリスク評価を実施する義務）の充足に必要とされる合理的な協力および支援を顧客に提供するものとする。

DPA の別紙

本別紙は、本 DPA の一部を構成する。

別紙 I

A. 当事者のリスト

管理者である顧客と、処理者であるプロバイダとの間の本契約には、以下を含め、必要なすべての情報の記載が含まれている。

- 氏名（名称）、住所、担当者名、
- 地位および連絡先情報、
- これらの条項に基づき送信されるデータに関連する活動
- 署名および日付

B. 処理の説明

1. 個人データが処理されるデータ主体の類型

顧客が別段の規定をした場合を除き、処理対象となる個人データは、次の類型のデータ主体に関するものである。

- 顧客の従業員、委託先、ビジネス パートナー。

2. 処理される個人データの類型

顧客は、本サービスの使用ごとにデータの類型を決定する。処理対象となる個人データは、通常、以下のデータ類型に関するものである。

- 顧客の従業員、または顧客により、もしくは顧客に代わり個人情報が提供されるその他の第三者に関する雇用の詳細（これには、会社の名称および住所、役職、等級、人口統計データならびに所在地データが含まれる可能性がある）。
- 顧客のシステム、または顧客がプロバイダに提供したシステム（本契約に基づき購入された本サービスに関連するものであり、かつ本サービスの提供に必要なもの）に関するシステム情報（これには、ユーザーID およびパスワード、コンピュータおよびドメイン名、使用中のコンピュータまたはその他のデバイスの IP アドレス、GUID 番号または位置情報が含まれる可能性がある）。

本書に基づき処理される顧客の個人データは、過去、現在および将来におけるビジネス パートナーまたは当該ビジネス パートナーに関係するその他の個人に関するものである場合がある。

3. 機密データの処理（該当する場合）

顧客は、特別な類型の個人データ（センシティブ データ）が個々のケースごとに特定され、かつ、かかる特別な類型のデータが本サービスの対象に含まれることについて両当事者が合意した場合でなければ、特別な類型の個人データを提供してはならない。

4. 処理の頻度（例：データが単発的に処理されるか、継続的に処理されるか）

本サービスの利用期間中、継続的に処理される。

5. 処理の性質

a） ソフトウェア保守契約に基づく処理：プロバイダまたはその復処理者は、顧客が、本ソフトウェアが利用できないこと、または想定された通りに作動しないことを理由にサポート チケットを提出した場合に、サポートを提供する。プロバイダまたはその復処理者は、電話対応および基本的なトラブルシューティングを行い、追跡システムにおいてサポート チケットを管理する。

b） コンサルティング サービス契約に基づく処理：プロバイダまたはその復処理者は、サービス オーダーに従い本サービスを提供する。

c） SaaS ソフトウェア契約に基づく処理：顧客が購入した SaaS ソフトウェアの提供。

6. データ転送および追加処理の目的

プロバイダが処理する顧客の個人データは、以下の基本的な処理活動の対象となる。

a） 以下に記載された指示に従い、プロバイダの本サービスを提供すること、本契約に基づき SaaS ソフトウェアへのアクセス権および同ソフトウェアの便益を提供すること（該当する場合）、ならびに顧客の要求に応じ、顧客の特定の要件に従ってテクニカル サポートを提供すること（該当する場合）を目的に、個人データを使用すること。

b） 個人データの保管

c） データ送信のための個人データのコンピュータ処理

d） プロバイダの本サービスの一部として提供されるサービスの特性および機能（自動化、取引処理および機械学習を含む）の継続的な改善。

e） 本契約に基づく顧客の指示の実行。

SaaS ソフトウェアで保存されている個人データは、以下の追加的な処理活動の対象となる。

a） データ センター（マルチテナント アーキテクチャ）での個人データの保管。
b） SaaS ソフトウェアに保存されている顧客の個人データのバックアップおよび復元。
c） 個人データのコンピュータ処理（データ送信、データ検索、データ アクセスを含む）。
d） 顧客のユーザーへの連絡。
e） SaaS ソフトウェアの修正またはアップグレードのリリース、開発およびアップロード。
f） 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。
g） SaaS ソフトウェアの基礎的なインフラストラクチャおよびデータベースの監視、トラブルシューティングおよび管理。
h） 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。
i） 下記に記載されている指示に従い、適宜、データ主体の要請および要求に適切に対応および対処すること。

プロバイダは、製品の改善およびプロバイダの新製品および新サービスの開発に関連する目的のため、匿名化されたデータ（顧客の個人データではないが、顧客の個人データから派生したものである可能性がある）を使用することができる。

SaaS ソフトウェアの機能、同ソフトウェアによる個人データの取扱方法、およびデータ保存場所の詳細については、該当する製品ドキュメンテーションおよびセキュリティ ガイドに記載されている。

7. 個人データが保持される期間、または期間を定めることが不可能な場合は、当該期間を決定するために使用される基準

前述の個人データは、本 DPA の第 9 条に従い、顧客が本契約に基づき本サービスを利用する期間にわたり処理されるものとする。

8. （復）処理者への転送の場合は、処理の主題、性質および期間も明記すること。

EU SCC に関して、復処理者への転送は、本 DPA に規定されたものと同じ根拠で行われるものとする。

9. 指示、顧客およびプロバイダのコミットメント。

プロバイダは、顧客の個人データに関し、顧客から受領した、書面および文書による指示に従う。ただし、当該指示が以下の全部またはいずれかに該当するものとプロバイダが考える場合を除く。（1）法的に禁止されている、または適用されるデータ保護法に違反する結果となる可能性がある。（2）プロバイダの本サービスへの重大な変更を要する。（3）本契約の条項または本書に基づき販売された本サービスに関連するプロバイダのドキュメンテーションと矛盾する。上記に該当する場合、プロバイダは、当該指示に従うことができない旨をただちに顧客に通知するものとする。本契約、本 DPA およびプロバイダの関連ドキュメンテーションに記載された処理の記述は、顧客による指示とみなされるものとする。

別紙 II―技術的および組織的な対策の表明

プロバイダは、本書に基づき顧客の個人データを処理する際、セキュリティ サイト（本DPAの第3条（a）の定義による）に規定された適切な技術的および組織的対策を使用する。顧客は、本書で合意されたデータ保護の全体的レベルが著しく低下しない限り、顧客の個人データを保護するために講じる対策をプロバイダが変更することができることに同意する。