PSLT – On-demand Services for Marketo Engage (2020v1)

1. **Compliance with Applicable Rules.**

   1.1 Customer shall, and shall ensure all Users comply with Applicable Rules. "Applicable Rules" means any and all laws, guidelines, regulations, codes, rules, and the Adobe Acceptable Use Policy (available at https://www.adobe.com/legal/terms/aup.html or a successor website thereto) applicable to Customer's use of the Products and Services.

   1.2 Customer acknowledges Adobe is only acting as a "data processor" on behalf of Customer and Customer is the "data controller" or equivalent under applicable privacy and data protection laws (including the General Data Protection Regulation if Customer is a resident of the EU).

   1.3 Customer shall obtain all necessary clearances, consents and approvals from all individuals that Customer or its Users contact through, or resulting from, the use of the On-demand Services in accordance with Applicable Rules with respect to any data gathered by, incorporated into or uploaded through the On-demand Services.

2. **Documentation.** For the purposes of this PSLT, the term "Documentation", as such term is defined in the General Terms, also includes the applicable technical specification and usage documentation for the Products and Services made generally available on https://docs.marketo.com.

3. **Usage Rights.** Customer shall not use the On-demand Services in excess of the usage terms specified in the Sales Order (such usage terms, the "Usage Rights"). If Adobe determines Customer is exceeding its Usage Rights, Adobe will notify Customer in writing or by email identifying such Usage Rights overage, and Customer shall promptly bring its usage of the On-demand Services within the limits of such Usage Rights. If Customer fails to do so within 30 days, Adobe has the right to charge Customer, and Customer agrees to pay, the fees applicable to a higher usage tier, which will be co-termed with the License Term in the applicable Sales Order.

4. **Data Retention and Destruction.** Customer may delete or retain Customer Data during the License Term, subject to applicable Usage Rights. After termination of the Agreement, Adobe will irretrievably delete and destroy Customer Data and, if requested in writing, Adobe will certify to such destruction.

5. **Delivery Errors.** Adobe is not responsible for the non-delivery of email messages that occur due to email address errors, hard bounces, soft bounces, email filters of mail clients, email blacklists, and/or any other similar cause therefor. Any or all of the foregoing can also adversely impact Customer's email delivery performance in connection with Customer's use of the On-demand Services, and, in such case, Adobe shall not be liable to Customer or any third party for any such adverse impact.

6. **Professional Services Termination.** Adobe may terminate any Professional Services upon thirty (30) days' written notice to Customer if Customer's performance under any applicable Sales Order delays or prevents Adobe from performing its obligations in a timely or effective manner.

7. **License Restrictions.** In addition to the conditions of the licenses granted to Customer and the license restrictions set forth in the General Terms, Customer shall not, and shall ensure that Users do not use or access the Products and Services to build, support, and/or assist a third party in building or supporting products or services competitive to the On-demand Services. If Customer is licensing a HIPAA-ready deployment of the On-demand Services: (a) Customer may not integrate the On-demand Services with any non-HIPAA-ready Products and Services; and (b) Customer must purchase encryption for data at rest for the full License Term of all Sales Orders.

8. **Product Changes.** Adobe reserves the right to change or discontinue individual features within the On-demand Services. Customer will be notified of such changes or discontinuations via the On-demand Services portal.

9. Processing and Categories of Personal Data; Security of Processing.

9.1 Security Measures and Data Processing. Security Claims and Data Privacy Claims of the General Terms shall apply to Customer only to the extent Customer purchases, for an additional fee, high-grade encryption for data at rest for the full License Term of all of Customer's Sales Orders.

9.2 The DPA (if applicable) is hereby revised by adding the following at the end of Section 3 (Processing and Types of Personal data) thereof: "Solely with respect to the On-demand Services for Marketo Engage: (a) Adobe Processes all Customer Data that may contain Personal Data in the locations described in the "Marketo Sub-processor List" located at: https://documents.marketo.com/legal/sub-processor-list; and (b) the subject matter, nature and purpose of the data processing and the type of Personal Data and categories of data subjects are in accordance with the Agreement and as more specifically described in the applicable Documentation." Any references to the list of sub-processors in such DPA shall instead refer to the sub-processors on the Marketo Sub-processor List (as defined in the foregoing excerpt).

9.3 Any references in the DPA (if applicable) to "Adobe Inc.," "Adobe US," or "Adobe" under the EU – US Privacy Shield, Swiss – US Privacy Shield, and/or Standard Contractual Clauses shall instead refer to "Marketo, Inc."

9.4 Adobe has implemented and maintains technical and organizational measures to ensure a level of security of the processing of Customer Data with respect to Adobe's Marketo Engage Products and Services appropriate to the risk as set forth in the attached Marketo Engage Technical and Organizational Measures (the "Marketo Engage Technical and Security Measures"). Any references in the DPA (if applicable) to Adobe's technical and organizational measures shall instead refer to the Marketo Engage Technical and Security Measures.

Marketo Engage Technical and Organizational Measures

1. Security Controls and Safeguards

1.1. Adobe will comply with all applicable privacy and data security laws and regulations governing its use, processing and storage of Customer Data.

1.2. During the License Term, Adobe shall maintain a security program materially aligned with applicable industry standards designed to ensure the security, confidentiality, availability and integrity of Customer Data and protect against unauthorized disclosure or access of Customer Data. Such security program shall include the implementation of administrative, technical and physical safeguards appropriate for the type of information that Adobe processes and the need for security and confidentiality of such information.

1.3. Adobe implements controls aligned to industry standards intended to keep Customer Data secure and throughout the License Term shall maintain security measures designed to: (i) protect the security of Adobe systems which interact with Customer Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Adobe systems which interact with Customer Data and (iii) protect against unauthorized access to or use of Adobe systems which interact with Customer Data that could result in harm to Customer's Users of the On-demand Services.

1.4. Adobe maintains access controls which include, but are not limited to, the following:

1.4.1. Limiting access to its information systems and the facilities in which they are housed to properly authorized persons;
1.4.2. Access by Adobe personnel to Customer Data is removed upon termination of employment or a change in job status that results in the personnel no longer requiring access to Customer Data;
1.4.3. System passwords conform to strong password standards (9 characters minimum) that include length, complexity and expiration. A maximum of ten (10) password attempts can be made, after which access is blocked until the password is reset by authorized personnel. Password policies conform with NIST Special Publication 800-53; and
1.4.4. Limited access to its information systems using multifactor authentication.

1.5. All customer communications transmitted over the internet are encrypted. Adobe utilizes encryption on its own email servers to ensure point-to-point encryption via opportunistic TLS. Customer can elect, for an additional charge, to configure the On-demand Services to use encrypted channels for its own collection of data via landing pages and from user activity on Customer's web site. Customer may elect to apply high grade encryption to data at rest for an additional fee. All backups are encrypted with high-grade encryption.

1.6. Adobe monitors its network and production systems and implements and maintains security controls and procedures designed to prevent, detect and respond to identified threats and risks. Such monitoring and testing includes, but is not limited to, the following:

1.6.1. Employing an industry standard network intrusion detection system to monitor and block suspicious network traffic;
1.6.2. Reviewing access logs on servers and security events and retaining network security logs for 180 days;
1.6.3. Reviewing all access to production systems;
1.6.4. Performing network vulnerability assessments on a regular basis. Scans will be performed using industry standard scanning tools that identify application and hosting environment vulnerabilities. Adobe shall maintain a vulnerability remediation program; and
1.6.5. Engaging third parties to perform network penetration testing on at least an annual basis.

1.7. Adobe shall ensure that:

1.7.1. All endpoints run an anti-virus solution and apply timely signature updates; and
1.7.2. All critical, exploitable vulnerabilities are patched in a timely manner.

2. Uses and Disclosures of Customer Data. Adobe will not use or disclose Customer Data except as necessary to provide the On-demand Services or as otherwise set forth in the Agreement.

3. Security Breach Notification. Adobe shall notify Customer within seventy-two (72) hours of becoming aware of a confirmed unauthorized acquisition, destruction, loss, modification, use or disclosure of Customer Data ("Security Breach").

3.1. Adobe will investigate and initiate the reasonably necessary steps to eliminate or contain the exposures that led to such Security Breach.
3.2. Adobe will, as soon as reasonably practicable, provide Customer with a written description of the Security Breach and the mitigation steps taken by Adobe.

4. Audit Reports. Adobe will obtain attestation reports related to its information security program (SSAE 16, SOC 2 or an equivalent report) at least annually and keep such reports for at least three (3) years following each attestation.

5. Security Awareness and Training. Adobe requires at least annual security and privacy training for all personnel.

6. Business Continuity and Disaster Recovery

6.1. Adobe has policies and procedures in place for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic, and natural disaster) that could affect the availability, integrity or confidentiality of Customer Data or production systems that contain Customer Data or that would interrupt Adobe's ability to provide On-demand Services under the Agreement.

6.2. Adobe's data protection, high availability, and built-in redundancy are designed to ensure application availability and protect information from accidental loss or destruction. Adobe's Disaster Recovery plan incorporates geographic failover between its U.S. data centers. On-demand Service restoration is within commercially reasonable efforts and is performed in conjunction with a data center provider's ability to provide adequate infrastructure at the prevailing failover location.

6.3. Adobe relies on reputable data center providers' multiple levels of power redundancy, uninterrupted power supply (UPS) and backup power for Adobe's system containing Customer Data. The power systems of the data centers processing Customer Data are designed to run uninterrupted during a total utility power outage, with every server receiving conditioned UPS power. The UPS power subsystem is redundant, with instantaneous failover if the primary UPS fails. All Adobe data center providers are ISO 27001:2013 certified.

6.4. Data center facilities containing Customer Data have advanced fire suppression systems and redundant heating, ventilation and air conditioning systems providing appropriate and consistent airflow, temperature and humidity levels.

6.5. Backup and Recovery. Data center facilities in the U.S. utilize snapshot and data mirroring capabilities. The integrity of local backups is tested quarterly by restoring a complete database from a selected snapshot copy to test systems and validate the data integrity. Data in the UK data center facility is backed-up to tapes daily and data in the Australia data center is backed-up electronically daily; the backup processes for the UK and Australia data center facilities are tested quarterly. Backup data is not transferred across international borders.

6.6. Network and Storage Redundancy. The SaaS infrastructure is designed and built for high availability. All network devices, including firewalls, load balancers, and switches are fully redundant and highly-available. High availability for Internet connectivity is ensured by multiple connections in each data center to different ISPs.

1. 適用規則の遵守

1.1 お客様は、適用規則を遵守し、すべてのユーザーをして遵守させるものとします。「適用規則」とは、お客様による本製品および本サービスの使用に関連して適用されるすべての法律、ガイドライン、規制、法典、規則および利用規定（https://www.adobe.com/jp/legal/terms/aup.html またはその後継ウェブサイトにてご確認いただけます。）を意味します。

1.2 お客様は、アドビがお客様に代わる「データ処理者」としてのみ行動するものであり、お客様が「データ管理者」または適用されるプライバシー法令およびデータ保護法令（お客様が EU の居住者の場合、EU 一般データ保護規則を含みます）に基づく同等の者であることを了承します。

1.3 お客様は、オンデマンドサービスを通じて収集され、これに組み込まれ、またはこれを通じてアップロードされるあらゆるデータについて、適用規則に従い、オンデマンドサービスの使用を通じて、またはその結果としてお客様またはそのユーザーがコンタクトしたすべての個人から必要な許可、同意および承認を取得するものとします。

2. **ドキュメンテーション**：本 PSLT において、「ドキュメンテーション」（基本利用条件で定義されます。）には、https://docs.marketo.com において公開されている、本製品および本サービスについて適用される技術的仕様および利用に関する文書も含むものとします。

3. **本利用権**：お客様は、セールスオーダーに記載された利用条件（以下当該利用条件を「本利用権」といいます。）を逸脱してオンデマンドサービスを利用しないものとします。お客様が本利用権を逸脱しているとアドビが判断した場合、アドビは、お客様に対して書面または電子メールにより当該本利用権の逸脱を特定して通知するものとし、お客様は、速やかに、お客様によるオンデマンドサービスの利用を本利用権の範囲内に収めるものとします。お客様が 30 日以内にこれを行わない場合、アドビは、該当するより高い利用レベル相当の料金の請求をお客様に対して行うことができ、お客様は、これに従い支払うことに同意し、該当するセールスオーダーに記載されるライセンス期間の適用を受けるものとします。

4. **データの保存および破棄**：お客様は、適用される本利用権に従い、ライセンス期間中お客様データを破棄または保存することができます。本契約が終了した後に、アドビは、お客様データを回復不能となるよう削除および破棄し、書面で要求された場合、かかる破棄を書面で認証します。

5. **配信エラー**：アドビは、電子メールアドレスの誤り、ハードバウンス、ソフトバウンス、メールクライアントの電子メールフィルター、電子メールブラックリストおよび／またはこれらに類似する原因によって発生する電子メールメッセージの不達について責任を負いません。上記いずれかまたはすべての原因は、お客様によるオンデマンドサービスの利用に関連してお客様の電子メール配信パフォーマンスにも悪影響を与えることがあり、この場合、アドビは、当該悪影響についてお客様または第三者に対して責任を負いません。

6. **プロフェッショナルサービスの解約**：アドビは、適用されるセールスオーダーに基づくお客様の履行が遅延し、または当該お客様の履行がアドビによる適時もしくは効果的な態様での義務の履行を妨げた場合、お客様に対して 30 日前までに書面通知を行うことにより、プロフェッショナルサービスを解約することができます。

7. **ライセンスの制限事項**：お客様に付与されたライセンスに係る条件および基本利用条件に定めるライセンスの制限事項に加えて、お客様は、オンデマンドサービスと競合する製品もしくはサービスを構築、サポートするために、および/またはこれを構築もしくはサポートする第三者を支援するために、本製品および本サービスを使用し、もしくはこれにアクセスしないものとし、ユーザーにさせないものとします。お客様が HIPAA 対応のオンデマンドサービスをデプロイするライセンスを取得している場合、(a)お客様は、オンデマンドサービスを非 HIPAA 対応の本製品および本サービスと統合してはならず、(b)お客様は、すべてのセールスオーダーの全ライセンス期間について保存データの暗号化を購入しなければならないものとします。

8. **製品の変更**：アドビは、オンデマンドサービスの中の個別の機能を変更または中止する権利を留保します。当該変更または中止については、オンデマンドサービスポータルを介してお客様に通知されます。

9. **個人データの処理および分類／処理についてのセキュリティ**：

9.1 セキュリティ対策およびデータ処理：基本利用条件におけるセキュリティ関連申立ておよびデータプライバシー関連申立ては、お客様が、追加料金を支払い、お客様のセールスオーダーのライセンス期間の全期間を通じて保存データについての高度な暗号化機能を購入した場合に限り、適用されるものとします。

9.2 データ処理覚書（適用がある場合）は、当該覚書の第 3 条（個人データの処理および種類）の末尾に以下を追加することにより修正されるものとします。「Marketo Engage のオンデマンドサービスに関する場合に限り、(a) アドビは、個人データを含む可能性のあるすべてのお客様データを、https://documents.marketo.com/legal/sub-processor-list にある「マルケト再委託先リスト」に記載された場所で処理し、また、(b)データ処理の主題、性質および目的ならびに個人データの種類およびデータ主体の分類は、本契約に従い、適用のあるドキュメンテーションにおいてより具体的に説明されるものとします。」当該データ処理覚書中の再委託先リストとは、マルケト再委託先リスト（上記引用箇所での定義に従います。）内の再委託先を指すものとします。

9.3 EU-米国間プライバシーシールド、スイス-米国間プライバシーシールドおよび／または標準的契約条項の下におけるデータ処理覚書（適用がある場合）中の「Adobe Inc.」、「Adobe US」または「Adobe」とは、「Marketo, Inc.」を指すものとします。

9.4 アドビは、アドビの Marketo Engage 製品およびサービスに係るお客様データの処理について添付の Marketo Engage 技術的および組織的措置（以下「Marketo Engage Technical and Security Measures」といいます。）に記載されるリスクに適合するセキュリティ水準を確保するための、技術的および組織的な措置を講じ、維持しています。データ処理覚書（適用がある場合）中のアドビの技術的および組織的措置とは、Marketo Engage Technical and Security Measures を指すものとします。

Marketo Engage 技術的および組織的措置

1. セキュリティ管理および安全措置

1.1. アドビは、お客様データの利用、処理、および保存に適用されるすべてのプライバシーおよびデータ保護に関する法令を遵守します。

1.2. ライセンス期間中、アドビは、お客様データのセキュリティ、機密性、可用性、および完全性を確保し、お客様データを不正開示や不正アクセスから保護するよう策定された、適用される業界標準に実質的に適合するセキュリティプログラムを維持するものとします。このセキュリティプログラムは、アドビが処理する情報の種類ならびにかかる情報のセキュリティおよび機密の必要性に適した管理的、技術的および物理的な安全措置の実施を含むものとします。

1.3. アドビは、お客様データを安全に保つことを目的として業界標準に沿った管理を実施するものとし、ライセンス期間中、次の目的で策定されたセキュリティ対策を維持するものとします：(i)お客様データとやり取りするアドビのシステムのセキュリティの保護、(ii)お客様データとやり取りするアドビのシステムのセキュリティまたは完全性に対して予想される脅威または危険に対する防御、および(iii)オンデマンドサービスのお客様のユーザーに害を与える可能性のある、お客様データとやり取りするアドビのシステムへの不正アクセスまたは不正使用に対する防御。

1.4. アドビは、以下を含みますが、これらに限定されないアクセス管理を維持します。

1.4.1. 情報システムおよびそれらが設置される施設へのアクセスを適切に許可された者に制限すること。

1.4.2. 雇用の終了または職務の変更により、お客様データへのアクセスが不要となったアドビの人員によるお客様データへのアクセスを排除すること。

1.4.3. システム用のパスワードが、長さ、複雑さおよび有効期限等において高度なパスワード基準（最低9文字）に適合すること。最大10回のパスワード試行を可能とするが、それ以降は、権限のある担当者がパスワードをリセットするまでアクセスをブロックすること。パスワードポリシーが、NIST Special Publication（米国標準技術局特別出版）800-53 に適合すること。

1.4.4. 多要素認証を使用して、情報システムへのアクセスを制限すること。

1.5. インターネットを介して送信されるすべての顧客通信は暗号化されます。アドビは、opportunistic TLS による二地点間の暗号化を確保するために、自己の電子メールサーバーにおいて暗号を活用しています。お客様は、追加料金を支払うことにより、ランディングページおよびお客様のウェブサイト上のユーザーの活動から自らがデータを収集するために暗号化されたチャネルを使用するよう、オンデマンドサービスを設定することを選択できます。お客様は、追加料金を支払うことにより、保存データに高度な暗号を適用することを選択できます。すべてのバックアップは高度な暗号で暗号化されています。

1.6. アドビは、そのネットワークおよび実稼働システムを監視し、また、特定された脅威およびリスクを防止し、検出し、かつこれらに対応するために策定されたセキュリティ管理および手順を実施し、維持します。かかる監視およびテストは、以下を含みますが、これらに限定されません。

1.6.1. 疑わしいネットワークトラフィックを監視およびブロックするために、業界標準のネットワーク侵入検知システムを採用すること。

1.6.2. サーバー上およびセキュリティイベントのアクセスログを確認し、ネットワークセキュリティログを 180 日間保持すること。

1.6.3. 実稼働システムへのすべてのアクセスを確認すること。

1.6.4. ネットワークの脆弱性評価を定期的に行なうこと。スキャンは、アプリケーションおよびホスティング環境の脆弱性を検知する業界標準のスキャンツールを使用して行なうこと。アドビは脆弱性改善プログラムを維持するものとします。

1.6.5. 第三者に委託して、最低年に 1 回のネットワーク侵入テストを行うこと。

1.7. アドビは、以下を確保するものとします。

1.7.1. すべてのエンドポイントにおいてウィルス対策ソリューションが稼働し、適時にシグネチャアップデートが適用されること。

1.7.2. すべての重大かつ攻撃され得る脆弱性に、適時にパッチが適用されること。

2. **お客様データの利用および開示**:アドビは、オンデマンドサービスの提供に必要な場合または本契約に別途定める場合を除き、お客様データを利用または開示しません。

3. **セキュリティ侵害の通知**：アドビは、お客様データの不正な取得、破棄、喪失、変更、利用、または開示があったこと（以下「セキュリティ侵害」といいます。）を知った場合、72 時間以内にお客様に通知するものとします。

3.1. アドビは、調査を実施し、かかるセキュリティ侵害の原因となった露出を除去または阻止するために合理的に必要な措置を開始ます。

3.2. アドビは、合理的に実行可能な限り速やかに、セキュリティ侵害およびアドビが実施した対応策を説明した書面をお客様に提供します。

4. **監査報告書**:アドビは、情報セキュリティプログラムに関する認証報告書（SSAE 16、SOC 2 または同等の報告書）を少なくとも年に 1 回取得し、かかる報告書を各々認証の時から少なくとも 3 年間保管します。

5. **セキュリティ周知およびトレーニング**:アドビは、すべての人員に対して少なくとも年に 1 回のセキュリティおよびプライバシーのトレーニングを義務付けます。

6. **ビジネス継続性および災害復旧**

6.1. アドビは、お客様データもしくはお客様データを含む実稼働システムの可用性、完全性、もしくは機密性に影響を与え得る、または本契約に基づいてアドビがオンデマンドサービスを提供することに支障をきたし得る緊急事態もしくはその他の事象（例えば、火災、破壊行為、システム障害、パンデミック、および自然災害）に対応するための方針および手順を整備しています。

6.2. アドビのデータ保護、高可用性、および冗長構造は、アプリケーションの可用性を確保し、情報の偶発的な喪失または破壊を防ぐように設計されています。アドビの災害復旧計画には、米国のデータセンター間の地理的フェイルオーバーが含まれています。オンデマンドサービスの復旧は、商業的に合理的な努力の範囲内で行われ、関連するフェイルオーバー箇所に適切なインフラを提供するデータセンタープロバイダーの能力と連動して行われます。

6.3. アドビは、お客様データを含むアドビのシステムについて、信頼できるデータセンタープロバイダーの複数層の電力冗長、連続電力供給（UPS）、および非常用電源に依拠しています。お客様データを処理するデータセンターの電力システムは、完全な公共停電の際にも中断なく稼働し、すべてのサーバーが準備された UPS 電力の供給を受け受けられるように設計されています。UPS 電力サブシステムは冗長であり、主力 UPS が停止した場合には瞬時にフェイルオーバーします。すべてのアドビのデータセンタープロバイダーは、ISO 27001：2013 の認定を受けています。

6.4. お客様データを保管するデータセンター施設は、高度な防火システムならびに適切で安定した空気の流れ、温度および湿度レベルを提供する重複した暖房、換気および空調システムを装備しています。

6.5. バックアップおよび復元：米国のデータセンター施設は、スナップショットおよびデータミラーリング技術を採用しています。ローカルにおけるバックアップの完全性は、システムをテストし、データの完全性を確認するための選択されたスナップショットコピーから完全なデータベースを回復させることにより、四半期毎にテストされます。イギリスのデータセンター施設のデータは毎日テープにバックアップされ、オーストラリアのデータセンターのデータは毎日電子的にバックアップされます。イギリスおよびオーストラリアのデータセンター施設のバックアップ手順は、四半期ごとにテストされます。バックアップデータは国境を越えて転送されません。

6.6. 7 ネットワークおよびストレージの冗長性：SaaS インフラは、高可用性を有するよう設計および構築されています。ファイアウォール、負荷分散装置、およびスイッチを含むすべてのネットワークデバイスは、完全な冗長性および高可用性を有しています。インターネット接続の高可用性は、各データセンターが異なる ISP に複数接続することにより確保されています。