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 EU Directive 95/46 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.