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

1. **Einhaltung geltender Vorschriften.**

   1.1 Der Kunde hat geltende Vorschriften einzuhalten und sicherzustellen, dass alle Benutzer diese ebenfalls einhalten. „Geltende Vorschriften" bezeichnet jegliche und sämtliche Gesetze, Richtlinien, Vorschriften, Kodizes, Regeln sowie Adobes Richtlinie für zulässige Nutzung (einzusehen unter https://www.adobe.com/legal/terms/aup.html oder auf einer Nachfolgewebsite), die für die Nutzung der Produkte und Services durch den Kunden gelten.

   1.2 Der Kunde bestätigt, dass Adobe nur als „Auftragsverarbeiter" im Auftrag des Kunden handelt und dass der Kunde der „Datenverantwortliche" oder Entsprechung laut anwendbarem Datenschutzrecht (einschließlich Datenschutz-Grundverordnung, falls der Kunde in der EU ansässig ist).

   1.3 Der Kunde hat alle erforderlichen Freigaben, Genehmigungen und Zustimmungen von allen Einzelpersonen einzuholen, die der Kunde oder dessen Benutzer über die oder infolge der Nutzung der On-demand Services gemäß geltenden Vorschriften im Hinblick auf Daten kontaktieren, die durch die On-demand Services gesammelt, in diese eingebunden oder über diese hochgeladen werden.

2. **Dokumentation.** Zum Zwecke dieser produktspezifischen Lizenzbedingungen umfasst der Begriff „Dokumentation", so wie dieser Begriff in den Allgemeinen Geschäftsbedingungen definiert ist, auch die jeweilige technische Spezifikations- und Nutzungsdokumentation für die Produkte und Services, die unter https://docs.marketo.com allgemein verfügbar gemacht werden.

3. **Nutzungsrechte.** Der Kunde hat die On-demand Services nicht in einem Umfang zu nutzen, der die im Auftrag angegebenen Nutzungsbedingungen überschreitet (diese Nutzungsbedingungen werden als die „Nutzungsrechte" bezeichnet). Falls Adobe feststellt, dass der Kunde seine Nutzungsrechte überschreitet, wird Adobe dies dem Kunden schriftlich oder per E-Mail mitteilen, eine solche Überschreitung der Nutzungsrechte benennen und der Kunde hat unverzüglich seine Nutzung der On-demand Services unter die Grenzen solcher Nutzungsrechte zu bringen. Falls der Kunde dies nicht innerhalb von 30 Tagen tut, hat Adobe das Recht, dem Kunden die für eine höhere Nutzungsstufe geltenden Gebühren zu berechnen (was mit der gleichen Laufzeit wie der Lizenzdauer in den jeweiligen Auftrag aufgenommen wird) und der Kunde vereinbart, diese Gebühren zu bezahlen.

4. **Aufbewahrung und Vernichtung von Daten.** Der Kunde darf Kundendaten während der Lizenzdauer nach Maßgabe geltender Nutzungsrechte löschen oder aufbewahren. Nach Beendigung des Vertrages wird Adobe Kundendaten unwiederbringlich löschen und vernichten und - falls dies schriftlich angefordert wurde - wird Adobe eine solche Vernichtung bestätigen.

5. **Lieferfehler.** Adobe ist nicht für die Nichtlieferung von E-Mail-Nachrichten aufgrund von E-Mail-Adressfehlern, Hard-Bounces, Soft-Bounces, E-Mail-Filtern von Mail-Clients, E-Mail-Sperrlisten und/oder anderen ähnlichen Gründen verantwortlich. Jegliche und sämtliche der vorstehenden Punkte können auch negative Auswirkungen auf die E-Mail-Auslieferung des Kunden im Zusammenhang mit der Nutzung der On-demand Services durch den Kunden haben und in einem solchen Fall haftet Adobe dem Kunden oder Dritten nicht für solche negativen Auswirkungen.

6. **Kündigung der Professional Services.** Adobe kann Professional Services schriftlich mit einer Frist von dreißig (30) Tagen gegenüber dem Kunden kündigen, falls die Leistung des Kunden laut des jeweiligen Auftrags Adobe davon abhält, ihre Pflichten fristgemäß oder effizient zu erfüllen oder zu Verzögerungen führt.

7. **Lizenzeinschränkungen.** Zusätzlich zu den Bedingungen der dem Kunden gewährten Lizenzen und den in den Allgemeinen Geschäftsbedingungen vorgesehenen Lizenzeinschränkungen wird der Kunde die Produkte und

Services nicht dazu nutzen oder auf diese zugreifen, um Produkte oder Services zu erstellen, zu unterstützen und/oder Dritten dabei zu helfen, Produkte oder Services zu erstellen oder zu unterstützen, die mit den On-demand Services in Wettbewerb stehen, und wird sicherstellen, dass Benutzer dies ebenfalls nicht tun. Falls der Kunde eine HIPAA-bereite Bereitstellung der On-demand Services lizenziert hat: (a) darf der Kunde die On-demand Services nicht mit nicht-HIPAA-bereiten Produkten und Services integrieren und (b) muss der Kunde Verschlüsselung für Daten bei der Speicherung für die gesamte Lizenzdauer sämtlicher Aufträge erwerben.

**8. Produktänderungen.** Adobe behält sich das Recht vor, einzelne Funktionen innerhalb der On-demand Services zu ändern oder einzustellen. Dem Kunden werden solche Änderungen oder Einstellungen über das On-demand Services-Portal mitgeteilt.

**9. Verarbeitung und Kategorien personenbezogener Daten, Sicherheit der Verarbeitung.**

9.1 Sicherheitsmaßnahmen und Datenverarbeitung. Sicherheitsansprüche und Datenschutzansprüche der Allgemeinen Geschäftsbedingungen gelten nur in dem Umfang für den Kunden, in dem der Kunde gegen eine zusätzliche Gebühr für die volle Lizenzdauer sämtlicher Aufträge des Kunden hochwertige Verschlüsselung für Daten bei der Speicherung erwirbt.

9.2 Die Datenschutzvereinbarung (falls vorhanden) wird hiermit geändert, indem Folgendes am Ende von Abschnitt 3 derselben (Verarbeitung und Arten personenbezogener Daten) hinzugefügt wird: „Allein im Hinblick auf die On-demand Services für Marketo Engage: (a) Verarbeitet Adobe alle Kundendaten, die personenbezogene Daten enthalten könnten, an den Standorten, die in der „Marketo Datenunterverarbeiter-Liste“ unter https://documents.marketo.com/legal/sub-processor-list beschrieben sind, und (b) stehen Gegenstand, Art und Zweck der Datenverarbeitung und die Art von personenbezogenen Daten und Kategorien von Datenobjekten im Einklang mit der Vereinbarung und mit den näheren Einzelheiten der jeweiligen Dokumentation.“ Bezugnahmen auf die Liste von Datenunterverarbeitern in einer solchen Datenschutzvereinbarung beziehen sich stattdessen auf die Datenunterverarbeiter auf der Marketo Datenunterverarbeiter-Liste (wie im voranstehenden Auszug definiert).

9.3 Bezugnahmen in der Datenschutzvereinbarung (falls vorhanden) auf „Adobe Inc.“, „Adobe US“ oder „Adobe“ unter dem EU – US Privacy Shield, Swiss – US Privacy Shield und/oder Standardvertragsklauseln beziehen sich stattdessen auf „Marketo, Inc.“.

9.4 Adobe hat technische und organisatorische Maßnahmen umgesetzt und erhält diese aufrecht, um ein Sicherheitsniveau für die Verarbeitung von Kundendaten im Hinblick auf Adobes Marketo Engage Produkte und Services sicherzustellen, das dem Risiko angemessen ist, das in den beigefügten technischen und organisatorischen Maßnahmen von Marketo Engage (die „Technischen Maßnahmen und Sicherheitsmaßnahmen von Marketo Engage“) vorgesehen ist. Bezugnahmen in der Datenschutzvereinbarung (falls vorhanden) auf Adobes technische und organisatorische Maßnahmen beziehen sich stattdessen auf die Technischen Maßnahmen und Sicherheitsmaßnahmen von Marketo Engage.

**Technische und organisatorische Maßnahmen von Marketo Engage**

## 1. Sicherheitskontrollen und Schutzmaßnahmen

1.1. Adobe wird sämtliche geltenden Datenschutzgesetze und -vorschriften einhalten, die Adobes Nutzung, Verarbeitung und Speicherung von Kundendaten regeln.

1.2. Während der Lizenzdauer hat Adobe ein Sicherheitsprogramm aufrechtzuerhalten, das im Wesentlichen auf die jeweiligen Branchenstandards ausgerichtet ist und so konzipiert wurde, dass die Sicherheit, Vertraulichkeit, Verfügbarkeit und Integrität von Kundendaten sichergestellt sind und Schutz gegen unautorisierte Offenlegung von oder Zugriff auf Kundendaten besteht. Ein solches Sicherheitsprogramm hat die Umsetzung von administrativen, technischen und physischen Schutzmaßnahmen zu umfassen, die für die Art von Informationen, die Adobe verarbeitet, und den Bedarf an Sicherheit und Vertraulichkeit solcher Informationen geeignet sind.

1.3. Adobe setzt Kontrollen um, die auf Branchenstandards ausgerichtet sind, die dazu dienen, Kundendaten zu schützen, und wird während der gesamten Lizenzdauer Sicherheitsmaßnahmen aufrechterhalten, um (i) die Sicherheit von Adobe Systemen zu schützen, die mit Kundendaten interagieren, (ii) gegen voraussichtliche Bedrohungen oder Gefahren für die Sicherheit oder Integrität von Adobe-Systemen zu schützen, die mit Kundendaten interagieren, und (iii) gegen unautorisierten Zugriff auf oder Nutzung von Adobe-Systemen zu schützen, die mit Kundendaten interagieren, was zu Schäden für die Benutzer der On-demand Services des Kunden führen könnte.

1.4. Adobe unterhält Zugriffskontrollen, die Folgendes umfassen, jedoch nicht darauf beschränkt sind:

1.4.1. Beschränkung des Zugriffs auf Adobes Informationssysteme und die Einrichtungen, in denen sich diese befinden, auf ordnungsgemäß autorisierte Personen,
1.4.2. Zugriff durch Adobe-Personal auf Kundendaten wird bei Beendigung der Anstellung oder einer Änderung des Jobstatus, der dazu führt, dass das Personal nicht länger Zugriff auf Kundendaten benötigt, aufgehoben,
1.4.3. Systempasswörter entsprechen Standards für starke Passwörter (mindestens 9 Zeichen), die Länge, Komplexität und Ablauf umfassen. Maximal zehn (10) Passworteingabeversuche können unternommen werden; danach wird der Zugriff blockiert, bis das Passwort durch autorisiertes Personal zurückgesetzt wurde. Passwortrichtlinien entsprechen NIST-Sonderveröffentlichung 800-53 und
1.4.4. begrenzter Zugriff auf Adobes Informationssysteme unter Verwendung von mehrstufiger Authentifizierung.

1.5. Sämtliche Kommunikation des Kunden über das Internet wird verschlüsselt. Adobe setzt auf ihren eigenen E-Mail-Servern Verschlüsselung ein, um Punkt-zu-Punkt-Verschlüsselung per opportunistischer TLS sicherzustellen. Der Kunde kann gegen Aufpreis wählen, die On-demand Services so zu konfigurieren, dass sie für sein eigenes Sammeln von Daten über Landingpages und aus Benutzeraktivitäten auf der Website des Kunden verschlüsselte Kanäle verwenden. Der Kunde kann wählen, gegen Aufpreis eine hohe Verschlüsselungsstufe für Daten bei der Speicherung anzuwenden. Alle Backups werden mit hoher Verschlüsselungsstufe verschlüsselt.

1.6. Adobe überwacht ihr Netzwerk und Produktionssysteme und setzt Sicherheitskontrollen und -verfahren um und erhält diese aufrecht, die dazu entwickelt wurden, identifizierte Bedrohungen und Risiken zu verhindern, zu erkennen und darauf zu reagieren. Diese Überwachung und Tests umfassen, sind jedoch nicht beschränkt auf, Folgendes:

1.6.1. Einsatz eines branchenüblichen Netzwerk-Einbruchmeldesystems zur Überwachung und Blockierung verdächtigen Netzwerk-Traffics,

1.6.2. Prüfung von Zugriffsprotokollen auf Servern und von Sicherheitsereignissen und Aufbewahrung von Netzwerk-Sicherheitsprotokollen für 180 Tage,
1.6.3. Prüfung aller Zugriffe auf Produktionssysteme,
1.6.4. Durchführung regelmäßiger Netzwerk-Schwachstellenanalysen. Scans werden unter Verwendung branchenüblicher Scanwerkzeuge durchgeführt, die Schwachstellen von Anwendungs- und Hosting-Umgebung identifizieren. Adobe hat ein Programm zur Behebung von Schwachstellen zu unterhalten und
1.6.5. Beauftragung Dritter mit der Durchführung von Netzwerkeindringungstests, die mindestens einmal jährlich durchzuführen sind.

1.7. Adobe hat sicherzustellen, dass

1.7.1. alle Endpunkte über eine Antivirenlösung verfügen und zeitnahe Signatur-Updates anwenden sowie
1.7.2. alle kritischen, nutzbaren Schwachstellen zeitnah beseitigt werden.

**2. Verwendung und Offenlegung von Kundendaten.** Adobe wird Kundendaten nicht verwenden oder offenlegen, außer dies ist erforderlich, um die On-demand Services zu erbringen oder wie anderweitig im Vertrag vorgesehen.

**3. Mitteilung über Sicherheitsverstoß.** Adobe hat dem Kunden innerhalb von zweiundsiebzig (72) Stunden nach Kenntnis einer bestätigten nicht autorisierten Erlangung, Zerstörung, Verlustes, Änderung, Nutzung oder Offenlegung von Kundendaten („Sicherheitsverstoß“) Mitteilung zu machen.

3.1. Adobe wird angemessene erforderliche Schritte untersuchen und einleiten, um die Gefährdungen, die zu einem solchen Sicherheitsverstoß geführt haben, zu eliminieren oder einzudämmen.
3.2. Adobe wird dem Kunden, sobald dies angemessenerweise praktikabel ist, eine schriftliche Beschreibung des Sicherheitsverstoßes und der von Adobe unternommenen Schritte zur Abschwächung zukommen lassen.

**4. Prüfungsberichte.** Adobe wird mindestens einmal pro Jahr Bestätigungsberichte zu ihrem Informationssicherheitsprogramm (SSAE 16, SOC 2 oder ein vergleichbarer Bericht) einholen und wird solche Berichte für mindestens drei (3) Jahre nach einer jeden Bestätigung aufbewahren.

**5. Sicherheitsbewusstsein und -training.** Adobe erfordert mindestens einmal jährlich Sicherheits- und Datenschutztraining für das gesamte Personal.

**6. Geschäftskontinuität und Notfallwiederherstellung**

6.1. Adobe verfügt über Richtlinien und Verfahren, um auf einen Notfall oder ein anderes Ereignis zu reagieren (z. B. Brand, Vandalismus, Systemausfall, Pandemie und Naturkatastrophe), das Auswirkungen auf die Verfügbarkeit, die Integrität oder Vertraulichkeit von Kundendaten oder Produktionssystemen, die Kundendaten enthalten, haben könnte, oder das Adobes Befähigung zur Erbringung von On-demand Services gemäß dem Vertrag stören würde.

6.2. Adobes Datenschutz, hohe Verfügbarkeit und eingebaute Redundanz sind so gestaltet, dass sie die Anwendungsverfügbarkeit sicherstellen und Informationen vor versehentlichem Verlust oder Zerstörung schützen. Adobes Notfallplan umfasst eine geografischen Ausfallsicherung zwischen ihren US-Rechenzentren. Die Wiederherstellung des On-demand Service erfolgt innerhalb wirtschaftlich angemessener Anstrengungen und wird gemeinsam mit der Befähigung eines Rechenzentrumsbetreibers zur Erbringung einer ausreichenden Infrastruktur am vorherrschenden Ausfallsicherungsstandort durchgeführt.

6.3. Adobe baut auf die mehrfachen Stufen von Stromredundanz, ununterbrochener Stromversorgung (UPS) und Reservestrom namhafter Rechenzentrumsbetreiber für Adobes System, das Kundendaten enthält. Die Stromsysteme der Rechenzentren, die Kundendaten verarbeiten, sind so konzipiert, dass sie während eines totalen Stromausfalls ohne Unterbrechung laufen und jeder Server gleichmäßige UPS erhält. Das UPS-Untersystem ist redundant, mit sofortiger Ausfallsicherung, falls die primäre UPS ausfällt. Alle Adobe-Rechenzentrumsbetreiber sind nach ISO 27001:2013 zertifiziert.

6.4. Rechenzentrumseinrichtungen, die Kundendaten enthalten, verfügen über hochentwickelte Brandunterdrückungssysteme und redundante Heizungs-, Belüftungs- und Klimasysteme, die angemessenen und gleichmäßigen Luftstrom, Temperatur und Feuchtigkeitsgrade liefern.

6.5. Sicherung und Wiederherstellung. Rechenzentrumseinrichtungen in den USA verwenden Snapshot- und Datenspiegelungsmöglichkeiten. Die Integrität lokaler Backups wird vierteljährlich getestet, indem eine vollständige Datenbank aus einer ausgewählten Snapshotkopie wiederhergestellt wird, um Systeme zu testen und die Datenintegrität zu validieren. Daten in der UK-Rechenzentrumseinrichtung werden täglich auf Bändern gesichert und Daten im australischen Rechenzentrum werden täglich elektronisch gesichert. Die Sicherungsverfahren für die Rechenzentrumseinrichtungen in UK und Australien werden vierteljährlich getestet. Sicherungsdaten werden nicht über internationale Grenzen hinweg übertragen.

6.6. Netzwerk- und Speicherredundanz. Die SaaS-Infrastruktur wurde für hohe Verfügbarkeit konzipiert und erstellt. Alle Netzwerkgeräte, einschließlich Firewalls, Load Balancern und Schaltern, sind vollständig redundant und hochverfügbar. Eine hohe Verfügbarkeit für Internetanbindung ist durch mehrere Verbindungen mit verschiedenen ISPs in jedem Rechenzentrum sichergestellt.