PSLT – Real-time Customer Data Platform (2020v1)

1. **Pflichten des Kunden.** Der Kunde ist allein verantwortlich für:
   1.1 Sicherstellung, dass alle in Real-time Customer Data Platform aufgenommenen Daten XDM-Standards entsprechen,
   1.2 Sicherstellung, dass alle in Real-time Customer Data Platform aufgenommenen Daten mit dem/den entsprechenden DULE-Label(s) versehen worden sind,
   1.3 Sicherstellung, dass innerhalb von Real-time Customer Data Platform entsprechende Datennutzungsrichtlinien (z. B. auf Grundlage von Datenschutzerklärungen des Kunden, vertraglichen Rechten und zustimmungsbasierten Rechten) umgesetzt worden sind und durchgeführt werden, und
   1.4 Sicherstellung, dass die Privacy Service-API nur verwendet wird, um Datenzugriff, -korrektur und -löschungsanfragen zu verarbeiten, die von einzelnen Datensubjekten stammen.

   Adobe ist nicht für Ausfälle des Betriebs von Real-time Customer Data Platform verantwortlich, die durch das Unterlassen des Kunden, die in Ziffern 1.1 bis 1.3 oben aufgeführten Pflichten zu erfüllen, verursacht wurden.
2. **Aufbewahrung von Daten**
   2.1 **Profilservice.** Einem Profil beigefügte Verhaltensdaten/Zeitreihendaten können 30 Tage nach dem Datum der Hinzufügung zu einem Profil oder nach einem alternativen Zeitraum, der vom Kunden innerhalb von Real-time Customer Data Platform gewählt wurde, aus Real-time Customer Data Platform gelöscht werden.
   2.2 **Daten-See.** Im Daten-See gespeicherte Kundendaten werden aufbewahrt:
      (A) 7 Tage lang, um die Eingliederung von Kundendaten in die Profilservices zu ermöglichen; anschließend können sie dauerhaft gelöscht werden,
      (B) 180 Tage lang, um Nutzungsfälle im Zusammenhang mit Kunden-KI-Intelligent-Service-Training oder -Verarbeitung zu ermöglichen; anschließend können sie dauerhaft gelöscht werden, oder
      (C) bis sie vom Kunden gelöscht werden.
3. **Übermittelte Daten.** Auf Anforderung des Kunden wird Adobe im Auftrag des Kunden bestimmte übertragene Daten an eine Targeting-Plattform senden. Der Kunde gewährleistet, dass jegliche Verwendung oder Vermischung der übermittelten Daten (sei es vom Kunden, der Targeting-Plattform oder anderen Dritten) mit geltendem Recht, Richtlinien, Vorschriften, Kodizes, Bestimmungen und dem anerkannten Stand der Technik hinsichtlich Datennutzung und Datenschutz (wie z. B. den DAA-Praktiken der Selbstkontrolle, sofern diese einschlägig sind) im Einklang steht.
4. **Nutzung einer Targeting-Plattform.** Adobes Übertragung von übertragenen Daten auf eine Targeting-Plattform gewährt der Targeting-Plattform oder anderen dritten Parteien nicht das Recht, (i) auf Adobes Onlineberichtsschnittstelle oder -tools zuzugreifen oder (ii) Berichte zu erhalten. Adobe kontrolliert weder die Nutzung der übertragenen Daten durch den Kunden über die Targeting-Plattform noch die Zusammenfügung der übertragenen Daten mit anderen Daten durch den Kunden über die Technologie oder die Services der Targeting-Plattform und ist auch nicht dafür verantwortlich. Kunden, die sogenannte People-based Destinations verwenden, müssen (a) Adobe gehashte Identifikatoren zur Verfügung stellen und (b) erforderliche Genehmigungen von den Besuchern ihrer Site einholen (die ggfs. laut Gesetz oder Branchenrichtlinien erforderlich sind).
5. **Ad Targeting.** Hat der Kunde seinen Sitz in den Vereinigten Staaten oder verwendet er die On-demand Services auf Kunden-Sites, die sich an Besucher aus den Vereinigten Staaten richten, hat der Kunde – soweit anwendbar – die DAA Selbstregulierungsprinzipien im Zusammenhang mit der Verwendung der On-demand Services einzuhalten.
6. **Verbotene Daten.** Der Kunde muss sicherstellen, dass weder der Kunde noch eine Targeting-Plattform verbotene Daten mit geschützten Daten zusammenfügen oder anderweitig verbinden oder andere

Handlungen vornehmen, die geschützte Daten in verbotene Daten umwandeln würden. Der Kunde muss geschützte Daten innerhalb der On-demand Services ordnungsgemäß kennzeichnen und sicherstellen, dass Richtlinien festgelegt und ausgeführt werden, um die Zusammenfügung oder Verbindung von geschützten Daten und verbotenen Daten zu verhindern.

7. **Zusätzliche Ansprüche**. Die in den Allgemeinen Geschäftsbedingungen vorgesehene Schadloshaltung des Kunden gilt ebenfalls für Ansprüche Dritter, die sich auf die Nutzung, Anzeige, den Austausch oder die Übertragung von übertragenen Daten zwischen Targeting-Plattformen, Kunden und Adobe beziehen oder daraus entstehen. Die zusätzlichen Ansprüche in diesem Abschnitt werden als Datenschutzansprüche oder andere Ansprüche behandelt, wie in den anwendbaren Allgemeinen Geschäftsbedingungen beschrieben. Die Haftungsbeschränkungsbestimmung in den anwendbaren Allgemeinen Geschäftsbedingungen gilt nicht für Ansprüche Dritter, die gegen Adobe von Social-Media-Targeting-Plattformen (z. B. Facebook, Google, Twitter oder Amazon) geltend gemacht werden, die sich aus der Nutzung von Real-time Customer Data Platform durch den Kunden ergeben.

8. **Definitionen.**

8.1 „**DAA**“ bezeichnet die Digital Advertising Alliance.

8.2 „**Direkt Identifizierbare Informationen**“ bezeichnet Informationen, die verwendet werden können, um unmittelbar eine Einzelperson zu identifizieren, einschließlich stabile Identifikatoren.

8.3 „**Direkt identifizierbares Profil**“ bezeichnet ein zusammengeführtes Profil, das direkt identifizierbare Informationen enthält.

8.4 „**DULE**“ bezeichnet Adobes Governance-Framework für Datennutzung, Kennzeichnung und Durchsetzung.

8.5 „**People-based Destinations**“ bezeichnet auf Menschen basierte Targeting-Plattformen (z. B., soziale Netzwerke), welche die Nutzung von gehashten Identifikatoren erfordern.

8.6 „**Profil**“ bezeichnet einen Satz Informationen, der eine Einzelperson repräsentiert (einschließlich direkt identifizierbarer Profile und pseudonymer Profile), wie er im Profilservice präsentiert wird.

8.7 „**Verbotene Daten**“ bezeichnet Daten, die es Adobe gestatten würden, unmittelbar eine bestimmte natürliche Person (im Gegenteil zu deren Gerät) zu identifizieren, wie deren Telefonnummer, E-Mail-Adresse, behördliche Identifizierungsnummer, Name, Postanschrift.

8.8 „**Geschützte Daten**“ bezeichnet pseudonyme Profildaten,

(A) die für auf das Onlineverhalten ausgerichtete Werbung („Online Behavioral Advertising“ - laut Definition der DAA) genutzt werden sollen, oder

(B) die der Kunde (oder dessen dritte Datenanbieter) anderweitig als Daten identifiziert hat, die nicht mit verbotenen Daten zusammengefügt werden können.

8.9 „**Pseudonymes Profil**“ bezeichnet ein zusammengeführtes Profil, das keine direkt identifizierbaren Informationen enthält.

8.10 „**Stabiler Identifikator**“ bezeichnet einen Identifikator außer einer Cookie ID oder einer Geräte-ID.

8.11 „**Targeting-Plattform**“ bezeichnet eine Einheit (z. B. Demand-side Platform, Anzeigenserver oder Content Management Platform), die

(A)

(1) mit dem Kunden einen Vertrag hat, der diesem Unternehmen Zugriff auf die übermittelten Daten gibt und zu deren Verwendung berechtigt, oder

(2) eine Datenzugriffsvereinbarung mit Adobe abgeschlossen hat, um auf die übertragenen Daten, die im Auftrag und laut Anweisungen des Kunden gesendet worden sind, zuzugreifen und diese zu nutzen, und

(B) über eine aktive Integration mit Adobe zur Nutzung mit Real-time Customer Data Platform

verfügt.

Der Kunde bestätigt und vereinbart, dass Adobe die Verfügbarkeit von bestimmten Targeting-Plattformen nicht garantiert und auch nicht garantieren kann.

8.12 „**Übermittelte Daten**“ umfasst die Kundendaten, die in die On-demand Services importiert oder aus diesen exportiert werden.

8.13 „**XDM**“ bezeichnet das unter https://**github**.com/adobe/xdm dokumentierte Experience Data Model.