PSLT - Healthcare Shield for Platform-based Applications (2023v1)

1. **Customer Responsibilities.** Customer is solely responsible for:

   1.1 ensuring that Customer creates, receives, maintains, or transmits Permitted Health Data in compliance with all applicable laws, rules, guidelines, regulations, and codes;

   1.2 ensuring that Customer retains, exports, and deletes Permitted Health Data in compliance with any applicable laws, rules, guidelines, regulations, and codes;

   1.3 ensuring that Permitted Health Data is made available and incorporates any amendments in compliance with all applicable laws, rules, guidelines, regulations, and codes; and

   1.4 ensuring that Customer labels any Permitted Health Data using the Data Usage labels of: Permitted Sensitive Personal Data or Restricted Health Data.

   Adobe will not be responsible for any failure in the operation or security of the Platform-based Applications caused by Customer's failure to meet the obligations outlined in sections 1.1 to 1.4 above or caused by Customer Customizations.

2. **Data Retention.** If Customer is required to retain its data for a specific time, Customer must export its data from the Platform-based Applications where available prior to the data deletion storage limits set out in the applicable underlying Platform-ased Applications PSLTs and General Terms.

3. **Permitted Health Data**. Notwithstanding any restrictions on Sensitive Personal Data in the General Terms, Customer may use the Platform-based Applications in connection with Healthcare Shield to create, receive, maintain, or transmit to Adobe, Permitted Health Data, as defined in this PSLT, provided Customer has obtained all necessary permissions, consents, clearances, and authorization required under applicable law or regulation for such use, including marketing, and Customer's activities do not otherwise cause Adobe or Adobe's third party providers to violate any applicable law or regulation.

4. **Additional Claims**. Customer's indemnification obligations set forth in the General Terms will also apply to Customer's use, collection, transmission, and processing of Permitted Health Data (a) outside of the Platform Based Applications, and (b) in violation of applicable laws, rules, guidelines, regulations, and codes. The additional Claims in this section are treated as Data Privacy Claims or Other Claims as described in the applicable General Terms. The Limitation of Liability provision in the applicable General Terms does not apply to Customer's liability or obligations under this section.

5. **HIPAA.** If Customer is a Covered Entity or Business Associate under HIPAA,

   5.1 and is creating, receiving, maintaining, or transmitting Permitted Health Data through Platform-based Applications, Customer represents it has executed a BAA with Adobe and is licensing Healthcare Shield; and

   5.2 Customer may not use, ingest, collect, share, or integrate Permitted Sensitive Personal Data with any non-HIPAA-Ready Products and Services.

6. **Definitions.** All capitalized terms used herein and not defined below are defined in the Business Associate Agreement or applicable Sales Order.

   6.1 "**Platform-based Applications**" means the following: (i) Real-Time Customer Data Platform Prime or Ultimate (B2C Edition) and (B2P Edition - Consumer Audiences only); (ii) Adobe Journey Optimizer; (iii) Customer Journey Analytics, and (iv) Attribution AI.

6.2 "**HIPAA-Ready**" means the Adobe Products and Services: (1) listed on https://www.adobe.com/trust/compliance/hipaa-ready.html; and (2) that Customer is expressly authorized via a written Sales Order to use to create, receive, maintain, or transmit Permitted Sensitive Personal Data in accordance with the BAA and applicable Agreement.

6.3 "**Permitted Health Data**" means an individual's financial information, medical or health information, but specifically excluding substance abuse, mental, or genetic health records, health records of a minor, data collected in connection with the Centers for Medicare & Medicaid and Services ("CMS"), biometric data, full account number, full credit card numbers, government identifiers, and personal information of children protected under any child protection laws (such as the personal information defined under the U.S. Children's Online Privacy Act ("COPPA")).