US Privacy Addendum (CCPA/CPRA)

Version 1

> ***Template — pending legal review.*** *This addendum applies to customers and data subjects in the United States. English is the operative language.*

US State Privacy Addendum (CCPA/CPRA)

This addendum supplements the Data Processing Agreement for personal information governed by US state privacy laws — primarily the **California Consumer Privacy Act (CCPA)** as amended by the **California Privacy Rights Act (CPRA)** — and analogous laws in Virginia (VCDPA), Colorado (CPA), Connecticut and others. It does not replace the GDPR-based DPA, which continues to govern EU/EEA data.

1. Roles

For personal information that the Customer ("Business") makes available through the platform, **Fotosoft SA** acts as a **"Service Provider"** (CCPA) / **"Processor"** (other state laws). Fotosoft processes personal information only to provide the service under the Customer's instructions and the DPA.

2. Service-provider commitments

Fotosoft shall **not**:

- sell or share personal information;
- retain, use or disclose personal information for any purpose other than performing the service, or as otherwise permitted by the CCPA;
- combine the personal information with data from other sources, except as permitted by the CCPA;
- retain, use or disclose the information outside the direct business relationship.

Fotosoft certifies that it understands and will comply with these restrictions.

3. Consumer rights

Fotosoft assists the Customer in responding to consumer requests to **know, access, delete, correct, and opt out of sale/sharing**. Because Fotosoft does not sell or share personal information, no opt-out mechanism is required on its part.

4. Sub-processors

Fotosoft engages sub-processors (see the Sub-processors list) under written contracts imposing the same service-provider obligations.

5. Data location

Personal information is hosted **exclusively in Europe**; there is no transfer of personal information to the United States for storage. EU?US transfer frameworks (e.g. the EU-US Data Privacy Framework) are therefore not relied

upon for storage.

6. Security and deletion

Reasonable security measures apply as described in the TOMs; data is deleted within **30 days** of account termination.

> *Review note (EN): confirm the applicable US state thresholds and the exact "service provider"/"contractor" language with counsel before relying on this.*