SOVA SYSTEMS

Data Processing Agreement

Version 2026.1 · Effective May 2026

This Data Processing Agreement ("DPA") forms part of the Master Services Agreement, Order Form, or other written agreement (the "Agreement") between SOVA Systems, LLC, a California limited liability company ("SOVA"), and the customer entity that has executed the Agreement ("Customer"). This DPA reflects the parties' agreement with respect to SOVA's processing of Personal Data on Customer's behalf in connection with the SOVA Offerings.

This DPA is incorporated into and forms part of the Agreement when executed by Customer. Capitalized terms not defined in this DPA have the meanings given in the Agreement.

Conflict with the Agreement. In the event of any conflict between this DPA and the Agreement with respect to the processing of Personal Data, this DPA shall control. In all other respects, the Agreement controls.

Conflict with addenda. If Customer has executed the Biometric Addendum or the EU/UK Data Transfer Addendum referenced in this DPA, the terms of those addenda control over this DPA with respect to their specific subject matter.

Contents

1. Definitions
2. Roles and Scope of Processing
3. Customer Instructions and Permitted Purpose
4. Confidentiality
5. Security Measures
6. Subprocessors
7. Data Subject Rights and Cooperation
8. Security Incident Notification
9. Audits and Compliance Verification
10. Data Deletion and Return
11. Aggregated and De-Identified Data
12. U.S. State Privacy Laws
13. International Data Transfers
14. Biometric Personal Information
15. AI and Machine Learning Processing
16. Limitation of Liability
17. Term and Survival
18. Miscellaneous

Annexes:

Annex 1 — Description of Processing

Annex 2 — Technical and Organizational Measures

Annex 3 — List of Subprocessors

1. Definitions

In this DPA, the following terms have the following meanings:

"Applicable Privacy Law" means all federal, state, local, and foreign data protection, privacy, and security laws and regulations applicable to a Party's processing of Personal Data, including without limitation the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), the Utah Consumer Privacy Act ("UCPA"), the Texas Data Privacy and Security Act ("TDPSA"), the Oregon Consumer Privacy Act, the Montana Consumer Data Privacy Act, and any successor or comparable laws in other U.S. states; and where the EU/UK Data Transfer Addendum has been executed, the GDPR and UK GDPR.

"Authorized Person" means any of SOVA's employees, contractors, or other personnel that SOVA has authorized to process Personal Data.

"Biometric Information" means Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person that allow or confirm the unique identification of that person, including without limitation facial recognition templates ("Facial Maps").

"Business" means as defined in the CCPA. Where Customer is the Business with respect to Personal Data processed by SOVA, references in this DPA to "controller" shall be deemed to refer to Customer in its capacity as the Business.

"Customer Data" means Personal Data contained in (i) any data Customer or its Authorized Users upload to or input into the SOVA Offerings, and (ii) data generated or collected in the course of Customer's configuration or use of the SOVA Offerings. Customer Data does not include Account Data.

"Account Data" means Personal Data SOVA processes about Customer's representatives, administrators, and billing contacts in connection with the formation, administration, billing, and support of Customer's account. SOVA is the controller (or, where applicable, the Business) of Account Data and processes it in accordance with SOVA's privacy notice, available at https://support.sovasystems.com/portal/en/kb/articles/sova-pricacy.

"Personal Data" means any information relating to an identified or identifiable natural person, including "personal information," "personally identifiable information," or any equivalent term as defined under Applicable Privacy Law.

"Process" means any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.

"Sale" means as defined in the CCPA. SOVA does not Sell Customer Data.

"Security Incident" means a confirmed breach of SOVA's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed by SOVA. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial-of-service attacks, or other network attacks on firewalls or networked systems.

"Sensitive Personal Information" means as defined in the CCPA, and including comparable categories under other Applicable Privacy Laws (such as "sensitive data" under VCDPA, CPA, CTDPA, and similar).

"Service Provider" means as defined in the CCPA. SOVA acts as a Service Provider to Customer with respect to Customer Data.

"Share" means as defined in the CCPA. SOVA does not Share Customer Data.

"Subprocessor" means any third-party processor engaged by SOVA to assist with the processing of Customer Data on Customer's behalf.

2. Roles and Scope of Processing

2.1 Roles. With respect to Customer Data, Customer is the controller (or Business, as applicable) and SOVA is the processor (or Service Provider, as applicable). With respect to Account Data, SOVA is the controller (or Business, as applicable) and processes Account Data in accordance with its own privacy notice.

2.2 Subject matter and duration. The subject matter, nature, purpose, and duration of SOVA's processing of Customer Data, the types of Personal Data processed, and the categories of data subjects are described in Annex 1.

2.3 Compliance with law. Each Party shall comply with the obligations applicable to it under Applicable Privacy Law in connection with the processing of Customer Data.

3. Customer Instructions and Permitted Purpose

3.1 Permitted Purpose. SOVA shall process Customer Data solely (a) as necessary to provide, maintain, secure, and support the SOVA Offerings in accordance with the Agreement; (b) on the documented instructions of Customer (including those set forth in the Agreement and this DPA); and (c) as required by Applicable Privacy Law (in which case SOVA shall, where legally permitted, inform Customer of that legal requirement before processing). Collectively, the foregoing constitutes the "Permitted Purpose."

3.2 Restrictions. SOVA shall not (a) Sell or Share Customer Data; (b) retain, use, or disclose Customer Data for any purpose other than the Permitted Purpose, including for any commercial purpose other than providing the SOVA Offerings; (c) retain, use, or disclose Customer Data outside of the direct business relationship between SOVA and Customer; or (d) combine Customer Data with personal information SOVA receives from or on behalf of any other person,

except as permitted by Applicable Privacy Law for a service provider performing a business purpose.

3.3 Notice of conflicting instructions. SOVA shall promptly notify Customer if, in SOVA's good faith opinion, an instruction from Customer infringes Applicable Privacy Law. Pending resolution, SOVA may suspend processing pursuant to the conflicting instruction without liability.

4. Confidentiality

SOVA shall ensure that each Authorized Person is subject to a written contractual or statutory duty of confidentiality with respect to Customer Data. SOVA shall limit access to Customer Data to those Authorized Persons who reasonably require such access for the Permitted Purpose.

5. Security Measures

5.1 Technical and organizational measures. SOVA shall implement and maintain appropriate technical and organizational measures designed to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The current measures are described in Annex 2 and shall be updated by SOVA from time to time consistent with the state of the art and the level of risk presented by the processing. In no event shall any update result in a material reduction of the level of security.

5.2 Personnel reliability. SOVA shall ensure that personnel with access to Customer Data are appropriately qualified and reliable, including, where permitted by law and consistent with the role, by conducting background checks.

6. Subprocessors

6.1 General authorization. Customer authorizes SOVA to engage Subprocessors to process Customer Data, subject to the conditions of this Section 6. The current list of Subprocessors is maintained at https://support.sovasystems.com/portal/en/kb/articles/subprocess (or such successor URL as SOVA may designate) and is reproduced as of the Effective Date in Annex 3.

6.2 Notice of new Subprocessors. SOVA shall provide notice of new Subprocessors at least thirty (30) days before authorizing any new Subprocessor to process Customer Data. Notice may be provided by updating the Subprocessor list at the URL above and notifying customers who have subscribed to update notifications, or by other reasonable means.

6.3 Objection. Customer may object to a new Subprocessor on reasonable, good-faith grounds related to data protection within thirty (30) days of notice. Upon objection, the Parties shall work in good faith for thirty (30) days to resolve Customer's concern, including by SOVA's offering of a commercially reasonable alternative. If no resolution is reached, Customer may, as Customer's sole remedy, terminate the affected SOVA Offering on thirty (30) days' written notice without penalty, and SOVA shall refund any pre-paid unused fees for the affected SOVA Offering for the period after termination.

6.4 Subprocessor obligations. SOVA shall enter into a written agreement with each Subprocessor that imposes data protection obligations on the Subprocessor that are no less protective than those imposed on SOVA under this DPA. SOVA remains liable for the acts and omissions of its Subprocessors with respect to Customer Data to the same extent SOVA would be liable if performing the services directly.

6.5 Operational support team. Customer acknowledges that SOVA's Subprocessors include a contracted offshore operational support firm (the "Operational Support Team") that handles routine technical support, operational tasks, and after-hours coverage. As described in the Agreement, the Operational Support Team's access is limited by role-based access control to operational functions and Customer organizational and contact records, and does not extend to visitor records, incident reports, biometric data, lost and found claimant data, persons-of-interest records, tour data, or other end-user Personal Data.

7. Data Subject Rights and Cooperation

7.1 Assistance. Taking into account the nature of the processing and the information available to SOVA, SOVA shall provide reasonable assistance to Customer (at Customer's cost, except where prohibited by Applicable Privacy Law) to enable Customer to respond to (a) requests from data subjects to exercise rights under Applicable Privacy Law (including rights of access, deletion, correction, portability, restriction of processing, and opt-out of Sale, Share, or targeted advertising); and (b) inquiries or complaints from regulators or other third parties relating to the processing of Customer Data.

7.2 Direct requests. If SOVA receives a request from a data subject relating to Customer Data, SOVA shall, except where prohibited by law, promptly redirect the data subject to Customer or notify Customer of the request without responding to its substance, and Customer shall be responsible for responding.

7.3 Data protection assessments. Upon Customer's reasonable written request, SOVA shall provide reasonable assistance (at Customer's cost) for Customer's preparation of any data protection assessment, data protection impact assessment, or transfer impact assessment required by Applicable Privacy Law in respect of Customer's use of the SOVA Offerings.

8. Security Incident Notification

8.1 Notification timing. SOVA shall notify Customer of any Security Incident affecting Customer Data without undue delay and in any event within seventy-two (72) hours after SOVA confirms the Security Incident.

8.2 Notification content. Each notification shall, to the extent then known and subject to legal or investigative restrictions, include: (a) a description of the nature of the Security Incident, including the categories and approximate number of data subjects and records affected; (b) the likely consequences of the Security Incident; (c) the measures taken or proposed to address the Security Incident and mitigate its possible adverse effects; and (d) a point of contact for further information. SOVA may provide information in stages as it becomes available.

8.3 Cooperation. SOVA shall cooperate with Customer in good faith and provide such information as Customer reasonably requires to fulfill its own notification, reporting, or remediation obligations under Applicable Privacy Law. Customer is solely responsible for assessing whether the facts of any Security Incident trigger notification obligations to data subjects, regulators, or others, and for issuing any such notifications.

8.4 No admission. SOVA's notification of, or response to, a Security Incident shall not be construed as an acknowledgment by SOVA of any liability or fault.

9. Audits and Compliance Verification

9.1 Documentation-based verification. SOVA makes available to Customer the audit cooperation rights set forth in the Agreement, which include: (a) SOVA's then-current Security Overview document; (b) summaries of infrastructure provider security certifications, currently including SOC 2 Type II and ISO 27001 attestations carried by SOVA's cloud infrastructure provider; (c) SOVA's own security framework attestations, if and when obtained; (d) summary reports from third-party penetration testing; and (e) SOVA's responses to standard vendor security questionnaires (such as CAIQ or HECVAT). Such information may be requested no more frequently than once per twelve (12) month period, except in connection with a Security Incident.

9.2 No on-site audits. SOVA shall not be required to provide direct access to its production systems, source code, or facilities. The compliance verification rights in Section 9.1 are Customer's exclusive audit rights under this DPA, and any further audit rights required by Applicable Privacy Law shall be exercised, where possible, by Customer's review of the documentation made available under Section 9.1.

9.3 Confidentiality of audit information. Information provided under this Section 9 is SOVA Confidential Information and shall be subject to the confidentiality provisions of the Agreement.

10. Data Deletion and Return

10.1 Deletion timing. Upon termination or expiration of the Agreement, SOVA shall, in accordance with the data export and disposal provisions of the Agreement, (a) provide Customer with the means to export Customer Data, and (b) delete Customer Data from production systems within the period specified in the Agreement and from backup systems in accordance with SOVA's standard backup rotation schedule.

10.2 Backups. Customer Data residing solely in backup systems shall be retained only for the duration of SOVA's standard backup rotation, after which it shall be deleted in the ordinary course. While retained, such Customer Data shall remain subject to the security and confidentiality obligations of this DPA and shall not be processed for any purpose other than disaster recovery.

10.3 Legal hold and process. SOVA may retain Customer Data beyond the deletion periods specified in this DPA to the extent reasonably required to comply with applicable law, legal process, a litigation hold, a pending or threatened claim of which SOVA has actual knowledge,

or a regulatory investigation. SOVA shall provide notice of any such retention and the basis for it, except where notice is prohibited. Data retained pursuant to this Section shall remain subject to this DPA and shall be deleted promptly upon expiration of the legal obligation.

11. Aggregated and De-Identified Data

11.1 Permitted use. SOVA may de-identify and aggregate Customer Data such that the resulting data does not identify any individual or Customer ("Aggregated Data") and may use Aggregated Data for the purposes of operating, securing, monitoring, supporting, troubleshooting, and improving the SOVA Offerings.

11.2 Restrictions. SOVA shall not (a) use Aggregated Data, Customer Data, or any data derived from Customer's use of the SOVA Offerings to train, fine-tune, or improve any artificial intelligence or machine learning model, except as expressly permitted by the Agreement (including any narrowly-scoped models trained exclusively for Customer's own benefit at Customer's written direction); (b) re-identify or attempt to re-identify Aggregated Data; or (c) disclose Aggregated Data in any manner that would permit re-identification.

12. U.S. State Privacy Laws

12.1 CCPA Service Provider terms. With respect to Personal Data subject to the CCPA, SOVA acts as a Service Provider to Customer in its capacity as a Business. SOVA: (a) shall not Sell or Share Personal Data; (b) shall not retain, use, or disclose Personal Data for any purpose other than the business purposes specified in the Agreement and this DPA, or as permitted by the CCPA; (c) shall not retain, use, or disclose Personal Data outside of the direct business relationship between the Parties; (d) shall not combine Personal Data with personal information from other sources except as permitted by the CCPA for a service provider performing a business purpose; and (e) certifies that it understands the restrictions in this Section and will comply with them.

12.2 Notice of inability to comply. SOVA shall notify Customer if SOVA determines that it can no longer meet its obligations under the CCPA. Customer may, upon reasonable notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data, including by suspending the affected SOVA Offering.

12.3 Other state laws. With respect to Personal Data subject to the VCDPA, CPA, CTDPA, UCPA, TDPSA, the Oregon Consumer Privacy Act, the Montana Consumer Data Privacy Act, or any successor or comparable U.S. state privacy law, SOVA acts as a processor to Customer in its capacity as a controller, and the obligations set forth in this DPA shall apply to such processing to the extent required by the applicable law. The Parties shall reasonably cooperate to address any specific requirements of such laws that are not otherwise addressed by this DPA.

12.4 Sensitive Personal Information. Where Customer instructs SOVA to process Sensitive Personal Information through the SOVA Offerings, Customer represents that it has provided all required notices and obtained all required consents under Applicable Privacy Law for such processing.

13. International Data Transfers

SOVA processes Customer Data in the United States. SOVA does not transfer Customer Data outside of the United States in the ordinary course of providing the SOVA Offerings.

13.1 EU/UK customers. Where Customer is an EU/UK controller, where Customer Data includes Personal Data of EU/UK data subjects, or where Applicable Privacy Law requires the use of Standard Contractual Clauses or comparable transfer mechanisms, the Parties shall execute the SOVA EU/UK Data Transfer Addendum, available at https://support.sovasystems.com (or such successor URL as SOVA may designate). The EU/UK Data Transfer Addendum incorporates the European Commission's 2021 Standard Contractual Clauses, the UK International Data Transfer Addendum, and references SOVA's commitments under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework as applicable. Until and unless the EU/UK Data Transfer Addendum is executed, no Personal Data subject to the GDPR or UK GDPR shall be processed under this DPA.

13.2 Operational Support Team location. The Operational Support Team described in Section 6.5 includes personnel located outside the United States. Customer's authorization of Subprocessors under Section 6 includes authorization for the Operational Support Team's access to Customer Data within the limited scope described in the Agreement.

14. Biometric Personal Information

14.1 Disabled by default. As set forth in the Agreement, biometric matching, facial recognition, and biometric template generation features of the SOVA Offerings are disabled by default and may be enabled only following execution of the SOVA Biometric Addendum.

14.2 Application of Biometric Addendum. Where Customer has executed the Biometric Addendum, the terms of that addendum supplement and, where in conflict, control over the terms of this DPA with respect to Biometric Information. Where Customer has not executed the Biometric Addendum, SOVA shall not process Biometric Information on Customer's behalf.

15. AI and Machine Learning Processing

15.1 Permitted AI processing. Where Customer enables AI features of the SOVA Offerings, SOVA may process Customer Data through artificial intelligence and machine learning systems for the operational purposes described in the Agreement, including incident report assistance, image analysis, and operational analytics.

15.2 PII Scrubbing. Where AI processing involves transmission of Customer Data to third-party AI service providers, SOVA shall apply automated preprocessing designed to remove or replace personally identifiable information with anonymized tokens prior to transmission, in accordance with the AI & Biometric Governance Policy set forth in the Agreement.

15.3 Third-party AI providers. SOVA shall maintain written agreements with all third-party AI service providers requiring (a) prohibition on use of Customer Data to train, fine-tune, or improve the provider's models; (b) transient processing and prompt deletion of inputs and

outputs; (c) confidentiality and security obligations no less protective than this DPA; and (d) breach notification obligations.

15.4 Automated decision-making. SOVA does not use AI features to make automated decisions producing legal or similarly significant effects on data subjects without human review. AI-generated outputs in the SOVA Offerings are designed to assist Authorized Users and require human review before operational use.

16. Limitation of Liability

Each Party's liability arising out of or relating to this DPA, whether in contract, tort, or otherwise, shall be subject to the limitations of liability set forth in the Agreement. Where the Agreement contains a Super Cap, Excluded Claims Cap, or comparable provisions applicable to claims relating to data privacy or security, those provisions shall apply to claims arising under this DPA.

17. Term and Survival

This DPA takes effect on the date Customer executes it (or the date Customer accepts it by clickthrough or other electronic means) and continues until SOVA's processing of Customer Data ceases. The provisions of this DPA that by their nature should survive termination — including without limitation Sections 4 (Confidentiality), 8 (Security Incident Notification), 10 (Data Deletion and Return), 11 (Aggregated and De-Identified Data), 16 (Limitation of Liability), and 18 (Miscellaneous) — shall survive termination of the Agreement.

18. Miscellaneous

18.1 Updates. SOVA may update this DPA from time to time to reflect changes in Applicable Privacy Law, in SOVA's processing practices, or in industry standards. SOVA shall provide Customer with notice of material updates at least thirty (30) days before the update takes effect, and Customer's continued use of the SOVA Offerings after the effective date constitutes acceptance of the updated DPA. If Customer reasonably objects to a material update, the Parties shall work in good faith to resolve the objection; if no resolution is reached, Customer may terminate the affected SOVA Offering on thirty (30) days' written notice.

18.2 Severability. If any provision of this DPA is held invalid or unenforceable by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect.

18.3 Governing law. This DPA is governed by the law specified in the Agreement.

18.4 No legal advice. This DPA does not constitute legal advice. Customer is responsible for its own assessment of the requirements applicable to its processing of Personal Data and is encouraged to consult with independent legal counsel.

Annex 1 — Description of Processing

Subject matter and duration

The subject matter of the processing is the provision of the SOVA Offerings under the Agreement. The processing continues for the duration of the Agreement and any wind-down period contemplated by the data deletion provisions of the Agreement and Section 10 of this DPA.

Nature and purpose

SOVA processes Customer Data to provide, maintain, secure, support, and improve the SOVA Offerings. Processing operations include collection, storage, organization, structuring, retrieval, transmission, display, analysis (including AI processing where enabled), backup, restoration, and deletion.

Categories of data subjects

- Customer's authorized users (security officers, supervisors, administrators, account managers)
- Visitors, deliveries, and vendors checked in through the SOVA Offerings
- Subjects of incident reports, persons-of-interest records, and lost-and-found claims (typically guests, employees, contractors, or members of the public present at Customer's facilities)
- Customer's clients and contacts (where Customer is itself a service provider deploying the SOVA Offerings at end-client facilities)

Categories of Personal Data

- Identifiers and contact information (name, phone number, mailing address; for visitors, also parsed identifying data from government identification barcodes)
- Photographs (visitor badge photographs; incident scene photographs)
- Operational records (incident reports, daily activity reports, tour data, persons-of-interest records, lost-and-found claims)
- Account credentials and authentication data
- Where biometric features are enabled under a Biometric Addendum: facial recognition templates
- Where Customer enables HIPAA-capable infrastructure under a Business Associate Agreement: Protected Health Information of the categories described in the BAA

SOVA does not process payment card information; payment processing is performed by SOVA's payment processor, identified in Annex 3.

Data not processed in the ordinary course

Driver's license images are not captured or stored. Government identification numbers parsed from barcodes are not retained beyond the visit. SOVA does not process special categories of Personal Data (such as data relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, health data, or data concerning a person's sex life or

sexual orientation) except to the extent such data may incidentally appear within Customer-uploaded incident narratives or photographs, which are governed by Customer's content responsibilities under the Agreement.

Annex 2 — Technical and Organizational Measures

SOVA implements and maintains the following technical and organizational measures to protect Customer Data. SOVA may update these measures from time to time, provided that no update results in a material reduction in security.

Access control

- Multi-factor authentication required for all SOVA administrative access, all elevated customer-facing access, and all access to source code repositories and cloud infrastructure consoles.
- Role-based access control limiting Authorized Persons to the minimum data necessary for their function.
- Audit logging of access to systems containing Customer Data, retained for not less than twelve (12) months.
- Segregation of operational support access from end-user Personal Data, as described in Section 6.5.

Encryption

- Encryption in transit using TLS 1.2 or higher.
- Encryption at rest using AES-256 or equivalent industry-standard algorithms, applied to production databases and backups.

Security operations

- Production infrastructure hosted on Amazon Web Services within the United States, leveraging AWS's SOC 2 Type II, ISO 27001, and other compliance certifications for the underlying infrastructure layer.
- Network segmentation between production, staging, and other environments.
- Annual third-party penetration testing of the SOVA Offerings, with remediation tracked to closure.
- Documented incident response plan, with named roles, pre-selected breach counsel and forensics resources, and periodic tabletop exercises.
- Vulnerability scanning and dependency monitoring on application code and infrastructure.

Data lifecycle

- Daily encrypted backups, retained for thirty (30) days, with documented restoration procedures.
- Data minimization through configurable retention policies for Personal Data-rich record types.
- Synthetic or masked data used in software development environments; production data access by development personnel limited to time-boxed, audit-logged exceptions.

Personnel

- Background checks for personnel with access to production systems, where permitted by applicable law.
- Confidentiality obligations imposed by written agreement on all Authorized Persons.
- Privacy and security training for personnel with access to Personal Data.

Vendor management

- Written agreements with all Subprocessors imposing data protection obligations no less protective than this DPA.
- Periodic review of Subprocessor compliance documentation, including SOC 2 reports and other third-party attestations where available.

Annex 3 — List of Subprocessors

The current list of Subprocessors is maintained at https://support.sovasystems.com/portal/en/kb/articles/subprocess (or such successor URL as SOVA may designate). The list is reproduced as of the Effective Date of this DPA below. SOVA shall provide notice of changes to the list in accordance with Section 6 of this DPA.

[Insert current Subprocessor list as published at the URL above. The list typically includes infrastructure providers (Amazon Web Services), payment processing (Stripe), shipping integration (Shippo), AI service providers, the Operational Support Team's contracting firm, and other Subprocessors as updated from time to time.]