DATA PROCESSING ADDENDUM

Addendum to the Transpara Master Software License Agreement — Version 2026.2 — Effective October 5, 2026

This Data Processing Addendum (this **"DPA"**) forms part of the Transpara Master Software License Agreement (the **"MSA"**) between the Transpara contracting entity identified in the applicable Order Form (**"Transpara"**) and Customer. This DPA applies whenever Transpara processes Personal Data on behalf of Customer in connection with the MSA. Capitalized terms used but not defined here have the meanings set forth in the MSA, the AI Addendum, or applicable Data Protection Laws.

Scope note (important): Transpara Software is installed and operated in the Customer Environment. As a general matter, Customer Data — including Personal Data processed in connection with Customer's industrial operations — does not leave the Customer Environment and is not accessed by Transpara. This DPA governs the limited categories of Personal Data that Transpara does process on Customer's behalf, primarily in connection with account administration, Support Services, and product telemetry. Personal Data that Customer chooses to submit to a Customer-Selected AI Model is processed under Customer's separate agreement with the Customer-Selected AI Model Provider; that provider is not a sub-processor of Transpara.

1. Definitions

Capitalized terms used but not defined in this DPA have the meanings given in the MSA, the AI Addendum, or applicable Data Protection Laws.

"Customer Personal Data" means Personal Data that Customer or its Authorized Users provide to Transpara, or that Transpara collects from the Software in the Customer Environment, in connection with Customer's use of the Software and Support Services. Customer Personal Data is described in Appendix 1.

"Data Protection Laws" means all laws and regulations applicable to the processing of Personal Data in connection with the Software, including (as applicable) the EU General Data Protection Regulation (Regulation (EU) 2016/679, the "EU GDPR"), the UK General Data Protection Regulation as incorporated into the law of the United Kingdom (the "UK GDPR"), the UK Data Protection Act 2018, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Texas Data Privacy and Security Act, and other applicable U.S. state privacy laws, the Swiss Federal Act on Data Protection, and other applicable data protection or privacy laws.

"Data Subject" means an identified or identifiable natural person to whom Customer Personal Data relates.

"Personal Data" has the meaning given under applicable Data Protection Laws (including "personal data" under the EU GDPR and "personal information" under the CCPA/CPRA).

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by Transpara.

"Process" or

"Processing" has the meaning given under applicable Data Protection Laws.

"Sub-processor" means any third party that Processes Customer Personal Data on behalf of Transpara, other than (i) Transpara's employees, contractors, or agents, and (ii) any Customer-Selected AI Model Provider (which is not a sub-processor of Transpara).

"Standard Contractual Clauses" or

"SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, together with the UK International Data Transfer Addendum or, as applicable, the Swiss Standard Contractual Clauses.

2. Roles and Scope

2.1 Roles.

With respect to Customer Personal Data, Customer is the controller (or processor on behalf of a third-party controller, as applicable) and Transpara is the processor (or sub-processor, as applicable) under EU GDPR and UK GDPR, the service provider or contractor (as applicable) under the CCPA/CPRA, and an analogous role under other Data Protection Laws.

2.2 On-Premise Architecture.

The Software is installed and operated in the Customer Environment. Customer Data, including any operational Personal Data, generally remains within the Customer Environment under Customer's control. Customer is the controller of such Personal Data and is responsible for compliance with all applicable Data Protection Laws with respect to such processing.

2.3 Scope of Transpara Processing.

Transpara Processes Customer Personal Data only in the limited categories and for the limited purposes described in Appendix 1. The categories include (a) account, billing, and contact information provided by Customer to administer the relationship; (b) information contained in Support Services tickets and communications initiated by Customer or its Authorized Users; (c) product telemetry and diagnostic data (which is typically aggregated and does not identify individual users, but may include user identifiers in some circumstances); and (d) any other Personal Data Customer expressly transmits to Transpara in writing for a specific purpose. Transpara does not Process operational Personal Data that remains in the Customer Environment.

2.4 Customer-Selected AI Model Providers.

Customer-Selected AI Model Providers are not Sub-processors of Transpara. Customer is responsible for entering into and complying with the data-processing arrangements required by Customer's agreement with each Customer-Selected AI Model Provider. Transpara has no obligation to procure data-protection terms from any Customer-Selected AI Model Provider.

3. Customer Instructions

3.1 Documented Instructions.

Transpara will Process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of Customer Personal Data to a third country, unless required to do so by applicable law. Customer's documented instructions include (a) this DPA, the MSA, and applicable Order Forms; (b) Customer's configuration of the Software, including any data submitted through the Software; and (c) Customer's reasonable written instructions delivered to legal@transpara.com.

3.2 Unlawful Instructions.

If Transpara reasonably believes that a Customer instruction violates applicable Data Protection Laws, Transpara will inform Customer in writing and may, at its option, suspend Processing under that instruction until the issue is resolved.

3.3 Legal Compulsion.

If Transpara is required by applicable law to Process Customer Personal Data otherwise than on Customer's instructions, Transpara will, to the extent permitted by law, inform Customer of that legal requirement before Processing.

4. Confidentiality and Personnel

4.1 Confidentiality.

Transpara will ensure that personnel authorized to Process Customer Personal Data are bound by appropriate confidentiality obligations, whether by contract, employment terms, professional duty, or statute.

4.2 Need-to-Know.

Transpara will limit access to Customer Personal Data to personnel who reasonably require access in order to perform Transpara's obligations under the MSA.

4.3 Training.

Transpara will provide appropriate training on data protection to personnel with access to Customer Personal Data.

5. Security Measures

5.1 Technical and Organizational Measures.

Transpara will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are described in Appendix 2 and may be updated by Transpara from time to time, provided that the level of protection does not materially decrease.

5.2 Encryption and Pseudonymization.

Where appropriate to the categories of Customer Personal Data and the risks of Processing, Transpara will employ encryption (in transit and at rest) and pseudonymization.

5.3 Ongoing Security Review.

Transpara will regularly test, assess, and evaluate the effectiveness of its technical and organizational measures.

6. Sub-processing

6.1 Authorization.

Customer authorizes Transpara to engage Sub-processors to Process Customer Personal Data, subject to this Section 6.

6.2 Current Sub-processors.

Transpara maintains a current list of its Sub-processors at *https://www.transpara.com/subprocessors* (the "Sub-processor List"). The Sub-processor List identifies, for each Sub-processor, the categories of Customer Personal Data Processed, the categories of Processing activity, and the location of Processing.

6.3 Notice of New Sub-processors.

Transpara will provide Customer with notice of any new Sub-processor (which may be by updating the Sub-processor List and providing email notification to the Notice Contact identified in the Order Form) at least thirty (30) days before authorizing the new Sub-processor to Process Customer Personal Data. Customer may object to the engagement of a new Sub-processor on reasonable data-protection grounds by providing written notice within the thirty (30) day notice period.

6.4 Effect of Objection.

If Customer objects to a new Sub-processor on reasonable data-protection grounds and the parties cannot reach a mutually acceptable resolution within thirty (30) days, Customer may, as its sole and exclusive remedy, terminate the affected Order Form on written notice to Transpara and receive a pro-rated refund of pre-paid Fees attributable to the unused remainder of the then-current Term.

6.5 Sub-processor Obligations.

Transpara will impose on each Sub-processor data-protection obligations that are no less protective than those set out in this DPA, including obligations to Process Customer Personal Data only on documented instructions, to maintain confidentiality, to implement appropriate security measures, and to assist with Data Subject rights and Personal Data Breach response. Transpara remains responsible to Customer for the acts and omissions of its Sub-processors as if they were Transpara's own.

7. Data Subject Rights

7.1 Assistance.

Taking into account the nature of the Processing, Transpara will assist Customer by appropriate technical and organizational measures, insofar as possible, to fulfill Customer's obligation to respond to requests from Data Subjects exercising rights under Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, objection, and rights regarding automated decision-making).

7.2 Direct Requests.

If Transpara receives a request directly from a Data Subject in respect of Customer Personal Data, Transpara will, unless legally prohibited, promptly forward the request to Customer and will not respond to the request itself except on Customer's documented instructions or as required by law.

7.3 Cost.

Transpara may charge a reasonable fee for assistance that is materially in excess of what is reasonably incidental to providing the Software and Support Services.

8. Personal Data Breach

8.1 Notification.

Transpara will notify Customer without undue delay, and in any event within seventy-two (72) hours after Transpara becomes aware, of any Personal Data Breach affecting Customer Personal Data. The notification will be sent to the Notice Contact identified in the Order Form (with a copy to Customer's data-protection officer or equivalent if known).

8.2 Information Provided.

The notification will include, to the extent then known: the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects affected and the categories and approximate number of records concerned); the likely consequences of the Personal Data Breach; the measures taken or proposed by Transpara to address the breach and mitigate its possible adverse effects; and the contact point at Transpara from which further information may be obtained. Transpara will provide subsequent information as it becomes available.

8.3 Cooperation.

Transpara will reasonably cooperate with Customer's investigation of, and response to, any Personal Data Breach, including by providing reasonable assistance in notifying supervisory authorities and Data Subjects where required by Data Protection Laws.

8.4 No Admission.

Notification of a Personal Data Breach is not an admission by Transpara of any fault or liability with respect to the Personal Data Breach.

9. International Data Transfers

9.1 EU/EEA Transfers.

Where Transpara Processes Customer Personal Data subject to the EU GDPR outside the European Economic Area, the parties agree that the SCCs (Module 2 — controller-to-processor, or Module 3 — processor-to-processor, as applicable based on Customer's role) are hereby incorporated into this DPA and apply to the transfer. The data-importer is Transpara LLC (or the Transpara entity identified in the Order Form), and the data-exporter is Customer (or Customer's Affiliate identified in the Order Form). The SCCs are completed as follows: the optional docking clause applies; Clause 9 Option 2 (general written authorization) applies for Sub-processor changes, with the thirty (30) day notice period set forth in Section 6.3; Clause 11 optional language is not included; Clause 17 selects the law of Ireland for purposes of the SCCs; Clause 18 selects the courts of Ireland; Annex I.A, I.B, and II are completed by reference to Appendix 1 and Appendix 2 of this DPA; Annex III is completed by reference to the Sub-processor List.

9.2 UK Transfers.

Where Transpara Processes Customer Personal Data subject to the UK GDPR, the UK International Data Transfer Addendum to the EU SCCs (as issued under section 119A of the Data Protection Act 2018) is hereby incorporated into this DPA and applies to the transfer.

9.3 Swiss Transfers.

Where Transpara Processes Customer Personal Data subject to the Swiss Federal Act on Data Protection, the SCCs apply with the following modifications: references to the EU GDPR are read as references to the Swiss FADP, references to the supervisory authority are read as references to the Federal Data Protection and Information Commissioner, and references to EU Member States are read as references to Switzerland.

9.4 Data Privacy Framework.

If Transpara becomes certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, or the Swiss-U.S. DPF (collectively, the "DPF"), the parties may, by written agreement, rely on the DPF as the transfer mechanism in lieu of (or in addition to) the SCCs. Transpara will notify Customer if it obtains DPF certification.

9.5 Customer Cooperation.

Customer will provide Transpara with all information reasonably necessary to enable Transpara to comply with the transfer mechanisms in this Section 9, including information regarding Customer's lawful basis for the transfer and any required notifications.

10. Audits

10.1 Records.

Transpara will maintain records of its Processing activities to the extent required by applicable Data Protection Laws.

10.2 Information.

On Customer's reasonable written request, Transpara will provide to Customer information reasonably necessary to demonstrate compliance with this DPA, including the latest available third-party audit reports, security certifications, or written attestations (subject to applicable confidentiality obligations).

10.3 On-Site Audits.

Where the information provided under Section 10.2 is not sufficient, and on at least thirty (30) days' prior written notice, Customer (or a qualified independent third-party auditor reasonably acceptable to Transpara and bound by confidentiality obligations no less protective than this DPA) may, at Customer's expense and during Transpara's normal business hours, conduct an audit of Transpara's data-protection compliance, limited to: (a) once per twelve (12) month period, (b) on a non-disruptive basis, and (c) excluding access to confidential information of other customers, source code, security keys, or other information whose disclosure would compromise security or the rights of third parties. Findings will be Transpara's Confidential Information.

10.4 Supervisory Authority.

Where required, Transpara will permit a supervisory authority to conduct an audit in accordance with applicable law.

11. Data Return and Deletion

11.1 Return or Deletion.

On termination or expiration of the MSA (or earlier on Customer's written request), Transpara will, at Customer's choice, delete or return all Customer Personal Data Processed by Transpara, subject to retention required by law and to copies maintained in routine backup systems that are subject to defined retention schedules and continue to be protected in accordance with this DPA until deleted.

11.2 Operational Data.

Customer Personal Data that resides in the Customer Environment (and that Transpara never received) is not within the scope of this Section 11; Customer is responsible for the retention, return, and deletion of Personal Data in the Customer Environment.

12. CCPA / CPRA Service Provider Terms

12.1 Service Provider Status.

With respect to Customer Personal Data subject to the CCPA/CPRA, Transpara is a "service provider" or "contractor" (as those terms are defined under the CCPA/CPRA), and Customer Personal Data is provided to Transpara solely for the purposes set out in this DPA and the MSA.

12.2 Restrictions.

Transpara will not: (a) sell or share Customer Personal Data (as those terms are defined under the CCPA/CPRA); (b) retain, use, or disclose Customer Personal Data for any purpose other than for the specific purposes set out in this DPA and the MSA, including for any commercial purpose other than providing the Software and Support Services; (c) retain, use, or disclose Customer Personal Data outside the direct business relationship between the parties; or (d) combine Customer Personal Data received from or on behalf of Customer with Personal Data that Transpara receives from or on behalf of any other person or collects from its own interactions with consumers, except as expressly permitted by the CCPA/CPRA.

12.3 Certification.

Transpara certifies that it understands the restrictions in Section 12.2 and will comply with them.

13. Liability

Each party's liability under this DPA is subject to the limitations of liability set forth in MSA Section 14, except that the carve-outs in MSA Section 14.3 apply to any breach of this DPA. To the extent a court of competent jurisdiction determines that the MSA's limitation of liability does not apply to claims arising under the SCCs, each party's liability under the SCCs is as set forth in the SCCs.

14. Order of Precedence

In the event of a conflict between this DPA and the MSA or any other document constituting the Agreement, this DPA controls solely with respect to the Processing of Customer Personal Data. In the event of a conflict between this DPA and the SCCs (or any other applicable transfer mechanism), the SCCs (or applicable transfer mechanism) control.

15. Signatures

This DPA is incorporated into and forms part of the MSA. Execution of the MSA or an Order Form constitutes execution of this DPA. Either party may also request a separately signed copy of this DPA, in which case the parties will execute it by authorized signature.

Appendix 1 — Details of Processing

A. Categories of Data Subjects:

- Customer's employees, contractors, and agents who act as Authorized Users of the Software or who interact with Transpara in connection with the MSA (including Customer's billing, notice, and technical contacts).
- Customer's employees, contractors, and agents who submit support tickets or other communications to Transpara.

B. Categories of Personal Data:

- Identification and contact data (e.g., name, business email, business phone, job title, business address).
- Account and authentication data (e.g., user IDs, role assignments, login times).
- Communications data (e.g., content of emails or support tickets initiated by Customer's personnel).
- Product telemetry and diagnostic data (e.g., software version, configuration, error logs, license metrics; may include user identifiers in some circumstances).
- Other Personal Data Customer expressly transmits to Transpara in writing for a specific purpose.

C. Special Categories of Personal Data (if any):

Transpara does not require any special category data (sensitive personal data, including racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic data, biometric data, health data, or data concerning sexual life or sexual orientation) for the operation of the Software or the provision of Support Services. Customer should not transmit special category data to Transpara, and Transpara will treat any inadvertent transmission of such data with the same care as other Customer Personal Data.

D. Frequency of Processing:

Continuous, on an as-needed basis, during the Term.

E. Nature of Processing:

- Account administration, billing, and contract management.
- Provision and improvement of the Software and Support Services.
- Responding to Customer's support requests and inquiries.
- Compliance with legal and regulatory obligations.
- Such other Processing as Customer expressly instructs in writing.

F. Purpose of Processing:

To perform Transpara's obligations to Customer under the MSA and Order Forms, and to comply with applicable law.

G. Duration:

For the duration of the MSA and any Order Form, and thereafter as required for legal, regulatory, or routine-backup retention purposes consistent with Section 11.

H. Transfers Outside the EEA, UK, or Switzerland (if applicable):

Transpara is headquartered in the United States. Customer Personal Data may be Processed in the United States and other jurisdictions where Transpara or its Sub-processors operate. International transfers are governed by Section 9 and the applicable transfer mechanism.

Appendix 2 — Technical and Organizational Security Measures

Transpara implements the following technical and organizational security measures, which may be updated from time to time provided the overall level of protection is not materially reduced:

A. Organizational Measures:

- Written information security policies covering access control, acceptable use, incident response, and data handling.
- Designated security responsibility within Transpara's leadership.
- Background checks for personnel with access to Customer Personal Data, as permitted by applicable law.
- Confidentiality obligations imposed on personnel and contractors with access to Customer Personal Data.
- Periodic security awareness training for personnel.
- Incident response plan with defined escalation paths.

B. Access Control:

- Role-based access controls based on the principle of least privilege.
- Strong authentication, including multi-factor authentication for administrative access to systems containing Customer Personal Data.
- Periodic review and timely revocation of access for personnel changes.
- Logging of administrative access to systems containing Customer Personal Data.

C. Encryption and Network Security:

- Encryption of Customer Personal Data in transit over public networks using industry-standard protocols (e.g., TLS 1.2 or higher).
- Encryption of Customer Personal Data at rest in Transpara systems, where appropriate to the categories of data and risk.
- Network segmentation and firewalls protecting systems containing Customer Personal Data.
- Vulnerability scanning and patching of Transpara systems.

D. Software Supply Chain:

- Software Bill of Materials (SBOM) maintained for the Software and made available to Customers.
- Secure software development practices, including code review and dependency scanning.

- Vulnerability disclosure policy and timely security patches as part of Support Services.

E. Physical Security:

- Transpara's corporate facilities and any third-party data centers used by Transpara employ industry-standard physical security controls, including access control and visitor management.

F. Business Continuity:

- Backups of Transpara-side systems containing Customer Personal Data, with documented retention and recovery procedures.
- Documented incident response and business continuity procedures.

G. Sub-processor Oversight:

- Written agreements with Sub-processors imposing data-protection obligations no less protective than this DPA.
- Periodic review of Sub-processor data-protection practices.

Note: Customer is solely responsible for the security of the Customer Environment, including the security of Customer Data and Customer Personal Data residing in the Customer Environment. The measures in this Appendix 2 cover Transpara-side Processing of the limited Customer Personal Data described in Appendix 1, and not Customer's operational systems or the Software as deployed in the Customer Environment.