DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is entered into by and between **Temperpack Technologies Inc.**, a Delaware corporation, with principal offices at 4101 Carolina Avenue, Richmond, Virginia 23222 U.S.A. ("**Company**"), and the customer entity agreeing to this DPA ("**Customer**").

This DPA is incorporated into and forms part of the applicable Terms and Conditions of Use, master services agreement, order form, subscription agreement, statement of work, or other written or electronic agreement governing Customer's access to and use of the Platform (the "**Principal Agreement**"). In the event of any conflict between this DPA and the Principal Agreement, this DPA shall control with respect to the Processing of Personal Data to the extent of such conflict.

---

1. DEFINITIONS

For purposes of this DPA, the following definitions apply:

1.1 "Affiliate"

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the relevant entity or the power to direct the management and policies of that entity.

1.2 "Applicable Data Protection Law"

"Applicable Data Protection Law" means all laws, regulations, and binding regulatory requirements applicable to the Processing of Personal Data under the Principal Agreement, including, where applicable, the GDPR, the UK GDPR, the Data Protection Act 2018, and applicable U.S. state privacy laws to the extent they impose processor or service-provider obligations on Company.

1.3 "Business Contact Data"

"Business Contact Data" means Personal Data relating to individual representatives, employees, agents, or contractors of Customer, including names, business email addresses, business phone numbers, titles, departments, and account credentials.

1.4 "Controller"

“Controller” means the entity that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Where Applicable Data Protection Law uses the term “Business,” “Controller” shall include “Business” to the extent applicable.

1.5 “Customer Personal Data”

“Customer Personal Data” means Personal Data Processed by Company on behalf of Customer under the Principal Agreement in Company’s role as Processor or service provider, and excludes Company Account Data, Usage Data Processed for Company’s own purposes, Security Data Processed for Company’s own purposes, and Derived Data.

1.6 “Data Subject”

“Data Subject” means an identified or identifiable natural person to whom Personal Data relates.

1.7 “Derived Data”

“Derived Data” means information, insights, analytics, reports, benchmarks, statistical models, trend data, algorithmic refinements, predictive outputs, de-identified data, aggregated data, and other information generated, inferred, transformed, or derived by or on behalf of Company from or through use, analysis, combination, or Processing of data, provided that Derived Data does not identify Customer or any Data Subject as such. For clarity, Derived Data includes de-identified and aggregated information and any improvements to Company’s algorithms, models, simulation methods, products, or services resulting from Processing activities.

1.8 “EEA”

“EEA” means the European Economic Area.

1.9 “GDPR”

“GDPR” means Regulation (EU) 2016/679.

1.10 “Personal Data”

“Personal Data” means any information relating to an identified or identifiable natural person, or any analogous concept under Applicable Data Protection Law, including “personal information” where such term is used under applicable law, but excluding information that is de-identified, anonymous, or aggregated such that it does not relate to an identified or identifiable individual.

1.11 “Process” or “Processing”

“Process” or “Processing” means any operation or set of operations performed on Personal Data, whether or not by automated means, including access, collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, deletion, destruction, combination, analysis, or other handling of Personal Data.

1.12 “Processor”

“Processor” means an entity that Processes Personal Data on behalf of a Controller. Where Applicable Data Protection Law uses the term “Service Provider” or “Contractor,” “Processor” shall include such terms to the extent applicable.

1.13 “Restricted Transfer”

“Restricted Transfer” means a transfer of Personal Data that is subject to restrictions under Applicable Data Protection Law relating to cross-border transfers.

1.14 “Security Incident”

“Security Incident” means a confirmed breach of Company’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data Processed by Company under this DPA. A Security Incident does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial-of-service attempts, malware alerts that are contained, or similar events.

1.15 “Standard Contractual Clauses” or “SCCs”

“Standard Contractual Clauses” or “SCCs” means the standard contractual clauses approved by the European Commission for transfers of personal data to third countries pursuant to GDPR Article 46, as amended, replaced, or superseded from time to time.

1.16 “Subprocessor”

“Subprocessor” means any third party or Affiliate engaged by or on behalf of Company to Process Customer Personal Data on behalf of Customer in connection with the Principal Agreement.

1.17 “Supervisory Authority”

“Supervisory Authority” means an independent public authority established under Applicable Data Protection Law with jurisdiction over the Processing of Personal Data.

1.18 “UK GDPR”

"UK GDPR" means the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

---

2. SCOPE AND ORDER OF PRECEDENCE

2.1 Scope

This DPA applies only to the extent Company Processes Customer Personal Data on behalf of Customer in connection with the services, software, tools, modules, analytics, interfaces, and associated offerings made available by Company under the Principal Agreement.

2.2 Role Allocation

The parties acknowledge and agree that, depending on the nature of the data and Processing activity:

(a) **Customer is Controller and Company is Processor** with respect to Customer Personal Data Processed by Company solely on Customer's behalf for the purpose of providing the Platform and related contracted services; and

(b) **Company is an independent Controller** with respect to Company Account Data, Business Contact Data Processed for Company's own account administration, billing, legal, compliance, security, fraud prevention, service integrity, product improvement, internal analytics, and Derived Data generation purposes.

2.3 No Restriction on Company Controller Activities

Nothing in this DPA restricts Company from Processing Personal Data as an independent Controller where Company has an independent legal basis and lawful purpose for such Processing under Applicable Data Protection Law, including for account administration, billing, compliance, security monitoring, fraud prevention, legal defense, internal product development, creation of de-identified or aggregated data, and development or refinement of Company's products, services, algorithms, or models, provided that such Processing is conducted in accordance with Applicable Data Protection Law.

2.4 Order of Precedence

In the event of conflict between the SCCs, if applicable, and this DPA, the SCCs shall control with respect to the subject matter of the transfer. In the event of conflict between this DPA and the Principal Agreement with respect to the Processing of Customer Personal Data, this DPA shall control.

3. NATURE OF PROCESSING; SUBJECT MATTER; DURATION

3.1 Subject Matter

The subject matter of the Processing under this DPA is the provision of the Platform and related services under the Principal Agreement, including without limitation customer account access, order-related interfaces, shipment-related tools, engineering or simulation tools, tracking-related functionality, analytics, support, and associated operational and administrative functions.

3.2 Nature of Processing

Company may Process Customer Personal Data by collecting, accessing, storing, organizing, structuring, transmitting, retrieving, consulting, analyzing, displaying, exporting, hosting, securing, deleting, and otherwise handling Customer Personal Data as necessary to provide the Platform and related services, maintain and secure the Platform, provide support, fulfill Customer instructions, and comply with Applicable Data Protection Law.

3.3 Purpose of Processing

The purpose of the Processing is to provide the Platform and related services to Customer, including enabling Customer-authorized users to access business information, input shipment or product parameters, receive model outputs or recommendations, review reports or account information, monitor permitted tracking or environmental data, and otherwise use the Platform in accordance with the Principal Agreement.

3.4 Duration

Company will Process Customer Personal Data for the duration of the Principal Agreement and thereafter only for so long as necessary to comply with its post-termination obligations under the Principal Agreement, this DPA, Applicable Data Protection Law, and Company's legitimate recordkeeping, backup, security, fraud prevention, legal defense, or compliance retention requirements.

3.5 Categories of Data Subjects

Data Subjects may include, as applicable:

a. Customer employees, contractors, and representatives;

b. Customer end users or authorized users;

c. business contacts associated with Customer's operations;

d. individuals identified in shipment, logistics, support, testing, or sample records; and

e. other individuals whose Personal Data is included in data submitted by or on behalf of Customer to the Platform.

3.6 Categories of Customer Personal Data

Customer Personal Data may include, as applicable:

a. names;

b. business email addresses;

c. business phone numbers;

d. company names;

e. job titles and departments;

f. account identifiers and authentication credentials;

g. shipment-related contact details;

h. support communications;

i. records associated with orders, samples, testing, or reports to the extent such records contain Personal Data; and

j. any other Personal Data submitted by or on behalf of Customer through the Platform.

3.7 Special Categories and Sensitive Data

Unless expressly agreed in writing by Company, Customer shall not submit to the Platform, and Company has no obligation to Process, any special categories of personal data, sensitive personal information, protected health information, biometric data, children's data, government-issued identification numbers, payment card data requiring PCI DSS treatment, or other regulated data requiring heightened protections under Applicable Data Protection Law. If Customer nevertheless submits such data in breach of this Section, Customer does so at its own risk and remains solely responsible for establishing a lawful basis for such submission and for notifying Company promptly so that Company may determine appropriate handling measures.

---

4. CUSTOMER INSTRUCTIONS

4.1 Processing on Documented Instructions

Company shall Process Customer Personal Data only on Customer's documented instructions, including as set forth in the Principal Agreement, this DPA, and Customer's use and configuration of the Platform, except where otherwise required by applicable law to which Company is subject. In such case, Company shall inform Customer of that legal requirement before Processing, unless applicable law prohibits such notice on important grounds of public interest.

4.2 Platform Functionality as Instruction

Customer acknowledges and agrees that Customer's configuration of the Platform, administrative settings, permissions, uploaded data, requests for support, and use of the Platform's features and functionality constitute documented instructions to Company.

4.3 Unlawful Instructions

Company shall have no obligation to follow instructions that, in Company's reasonable opinion, violate Applicable Data Protection Law, compromise the security, confidentiality, availability, or integrity of the Platform, or require material changes to the services not contemplated by the Principal Agreement. Company may suspend execution of such instructions pending clarification and shall not be liable for any resulting delay.

4.4 Customer Responsibility for Lawful Instructions

Customer represents, warrants, and covenants that it has provided and will continue to provide all notices and obtain all rights, permissions, and lawful bases necessary for Company to Process Customer Personal Data in accordance with Customer's instructions, the Principal Agreement, and this DPA.

---

5. CUSTOMER OBLIGATIONS

5.1 Compliance Responsibility

Customer is solely responsible for:

(a) determining whether the Platform is appropriate for Customer's intended use;

(b) ensuring that its instructions comply with Applicable Data Protection Law;

(c) ensuring that it has a lawful basis for the collection, disclosure, and Processing of Customer Personal Data;

(d) providing all required privacy notices to Data Subjects;

(e) responding to Data Subject requests, except to the extent Company's assistance is required under this DPA; and

(f) using the Platform in a manner consistent with Applicable Data Protection Law.

5.2 Accuracy and Minimization

Customer is responsible for the quality, accuracy, and legality of Customer Personal Data and for ensuring that only Customer Personal Data reasonably necessary for the intended business purpose is submitted to the Platform.

5.3 Restricted Data

Customer shall not submit restricted, high-risk, or specially regulated data unless expressly authorized in writing by Company and subject to additional contractual terms.

5.4 Customer Security Configuration

Customer is responsible for configuring user roles, access permissions, and account administration features made available by Company and for securing Customer's own systems, devices, credentials, and networks.

---

6. COMPANY PERSONNEL; CONFIDENTIALITY

6.1 Personnel Access Limitation

Company shall ensure that access to Customer Personal Data is limited to personnel, contractors, and subprocessors who require such access for the purposes of fulfilling Company's obligations under the Principal Agreement and this DPA or for Company's permitted Controller-side purposes described in Section 2.2(b), and whose access is subject to appropriate controls.

6.2 Confidentiality Obligations

Company shall ensure that any person authorized to Process Customer Personal Data is subject to a duty of confidentiality, whether by contract, professional obligation, or statutory duty, that survives the termination of that person's engagement or access.

6.3 Training and Awareness

Company shall maintain reasonable privacy and security awareness measures for personnel with access to Customer Personal Data appropriate to their role and responsibilities.

7. TECHNICAL AND ORGANIZATIONAL MEASURES

7.1 General Standard

Taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of Processing, and the risks to natural persons, Company shall implement and maintain commercially reasonable technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

7.2 Measures May Include

Without creating any warranty of invulnerability or absolute security, Company's measures may include, as appropriate to the Platform and Company's environment:

a. logical access controls and authentication mechanisms;

b. role-based access restrictions;

c. password or credential management procedures;

d. encryption in transit and, where appropriate, at rest;

e. network security controls;

f. logging and monitoring;

g. change management and patching practices;

h. backup and recovery procedures;

i. endpoint and malware protections;

j. incident response procedures;

k. vendor risk-management processes; and

l. physical safeguards for facilities under Company's control.

7.3 No Absolute Security Guarantee

Customer acknowledges that no security measure can guarantee absolute security and that Company does not warrant that the Platform will be immune from all security threats, vulnerabilities, or incidents. Company's obligations under this Section are obligations of means, not of result.

7.4 Review and Evolution

Customer acknowledges that Company may update, replace, or modify its technical and organizational measures from time to time, provided that such changes do not materially diminish the overall security of the Platform's Processing of Customer Personal Data.

---

8. SECURITY INCIDENTS

8.1 Notification Obligation

In the event of a Security Incident affecting Customer Personal Data, Company shall notify Customer without undue delay after becoming aware of the Security Incident.

8.2 Content of Notice

To the extent reasonably available at the time of notification, Company's notice shall include:

a. a description of the nature of the Security Incident;

b. the categories of Customer Personal Data affected;

c. the categories of affected Data Subjects, where known;

d. the likely consequences of the Security Incident, where reasonably ascertainable;

e. the measures taken or proposed to address and mitigate the Security Incident; and

f. contact information for follow-up.

8.3 Supplemental Information

Information may be provided in phases as it becomes available. Company's obligation to investigate or disclose shall not require disclosure of confidential information relating to other customers, compromise Company's security measures, or waive legal privilege.

8.4 No Admission

Notification of a Security Incident shall not be construed as an admission by Company of fault, liability, or wrongdoing.

8.5 Customer Responsibilities

Customer is solely responsible for determining whether to notify Data Subjects, Supervisory Authorities, regulators, customers, business partners, insurers, or other parties in connection with a Security Incident, except to the extent Applicable Data

Protection Law expressly requires Company to do so directly. Company shall provide reasonable cooperation to Customer in connection with Customer's notification obligations, at Customer's expense to the extent such cooperation exceeds Company's standard obligations under this DPA or arises from causes not attributable to Company's breach of this DPA.

---

9. SUBPROCESSORS

9.1 General Authorization

Customer hereby grants Company a general authorization to engage Subprocessors for the Processing of Customer Personal Data, provided that Company remains responsible for compliance with the obligations of this DPA to the extent required by Applicable Data Protection Law.

9.2 Subprocessor Conditions

Company shall impose on each Subprocessor, by written contract, data protection obligations materially protective of Customer Personal Data that are no less protective than those imposed on Company under this DPA, to the extent applicable to the nature of the services provided by that Subprocessor.

9.3 Current Subprocessors

Upon written request, Company shall make available to Customer information regarding categories of Subprocessors used in connection with the Platform, and may, at its discretion, maintain a list of significant Subprocessors or hosting regions.

9.4 Changes to Subprocessors

Company may add, replace, or remove Subprocessors from time to time in the ordinary course of business. Where Applicable Data Protection Law requires notice of new Subprocessors, Company shall provide notice by commercially reasonable means, which may include email, in-product notice, customer portal posting, or maintenance of an updated subprocessor list.

9.5 Objections

If Customer reasonably objects to a new Subprocessor on documented data protection grounds, Customer must notify Company in writing within ten (10) business days after the relevant notice. The parties shall discuss the objection in good faith. If Company cannot provide a commercially reasonable alternative and the objection is not resolved within a

reasonable period, Customer's sole and exclusive remedy shall be to terminate the affected services upon written notice, subject to the termination provisions of the Principal Agreement. Customer shall not withhold or delay payment or claim breach solely due to Company's use of a Subprocessor in compliance with this Section.

---

10. DATA SUBJECT REQUESTS

10.1 Customer Responsibility

As between the parties, Customer is responsible for responding to requests from Data Subjects to exercise rights under Applicable Data Protection Law, including rights of access, rectification, erasure, restriction, portability, objection, or similar rights.

10.2 Company Assistance

Taking into account the nature of the Processing, Company shall provide commercially reasonable assistance to Customer, through appropriate technical and organizational measures where possible, to enable Customer to respond to Data Subject requests insofar as Customer cannot reasonably fulfill such requests independently through the Platform or its own systems.

10.3 Direct Requests to Company

If Company receives a request directly from a Data Subject relating to Customer Personal Data for which Customer is the Controller, Company shall, to the extent legally permitted, either:

(a) direct the Data Subject to Customer; or
(b) notify Customer of the request and await Customer's instructions,

provided that Company shall not be obligated to respond directly to the Data Subject except as required by Applicable Data Protection Law.

10.4 Limitations

Company's assistance under this Section is limited to Customer Personal Data Processed by Company as Processor and does not require Company to disclose information that would reveal Company's confidential information, trade secrets, security architecture, or information relating to other customers, or to take action inconsistent with Applicable Data Protection Law.

---

11. DPIAS; PRIOR CONSULTATION; REGULATORY COOPERATION

11.1 Assistance with Assessments

To the extent required by Applicable Data Protection Law and taking into account the nature of the Processing and information available to Company, Company shall provide commercially reasonable assistance to Customer in connection with data protection impact assessments and prior consultations with Supervisory Authorities relating to Customer's use of the Platform, solely to the extent Customer cannot reasonably access the relevant information otherwise.

11.2 Scope Limitation

Company's obligation under this Section does not require Company to disclose information that would compromise Company's confidential information, internal security measures, trade secrets, or the rights of other customers, or to perform legal analysis for Customer.

11.3 Cost Allocation

Where such assistance requires material additional effort beyond Company's standard service commitments, the parties may agree that Customer will reimburse Company's reasonable costs.

---

12. RETURN AND DELETION OF CUSTOMER PERSONAL DATA

12.1 General Obligation

Upon termination or expiration of the Principal Agreement, and upon Customer's written request made within thirty (30) days after the effective date of such termination or expiration, Company shall use commercially reasonable efforts to delete or, where commercially feasible, return Customer Personal Data that Company holds solely in its capacity as Processor under this DPA, subject to the carve-outs in Sections 12.3 and 12.4 and Company's rights as an independent Controller set forth in Section 12.6. Company has no obligation to delete or return data it holds as an independent Controller, Derived Data, de-identified data, or any other data outside the scope of Company's Processor obligations. If Customer does not submit a written deletion or return request within thirty (30) days following termination or expiration, Company's obligation under this Section 12.1 shall be deemed satisfied and Company may retain such data in accordance with its standard retention practices and applicable law.

12.2 Method of Return

Where supported by the Platform or otherwise commercially reasonable, Company may permit Customer to retrieve Customer Personal Data during the term of the Principal Agreement or for a limited post-termination retrieval period.

12.3 Retained Copies

Notwithstanding the foregoing, Company may retain Customer Personal Data:

a. in backup systems until overwritten in the ordinary course;

b. as required by Applicable Data Protection Law;

c. as necessary to establish, exercise, or defend legal claims;

d. to comply with legal holds, audit obligations, or recordkeeping requirements; and

e. as part of security logs, incident records, fraud prevention records, or compliance archives.

12.4 Excluded Data

For avoidance of doubt, Company has no obligation to return or delete:

a. Derived Data;

b. de-identified or aggregated data;

c. system logs, diagnostic data, telemetry, or usage data retained for Company's legitimate business purposes as Controller;

d. information retained in immutable archives or backups until normal deletion cycles occur; or

e. data retained pursuant to a legal obligation or lawful exception.

12.5 Certification

Upon written request, Company may certify completion of deletion in a commercially reasonable manner, subject to the exclusions and limitations set forth in this DPA.

12.6 Company Independent Controller Retention Rights

Notwithstanding any other provision of this Section 12, Company shall have no obligation to return, export, or delete any data, information, or records that Company Processes as an independent Controller pursuant to Section 2.2(b) or Section 16 of this DPA, including Business Contact Data retained for account administration, billing, or relationship management; Usage Data, telemetry, logs, and diagnostic information retained for service

integrity, debugging, capacity planning, feature development, or internal analytics; security-related information retained for fraud prevention, intrusion detection, threat analysis, incident response, or legal defense; Derived Data; and de-identified or aggregated data. Company may retain all such data indefinitely and for any purpose consistent with Applicable Data Protection Law. Nothing in this DPA limits Company's rights as an independent Controller with respect to the foregoing categories of data.

---

13. AUDITS AND INFORMATION RIGHTS

13.1 Information Available

Company shall make available to Customer information reasonably necessary to demonstrate Company's compliance with this DPA, which may include summaries of security measures, relevant certifications or attestations if available, responses to security questionnaires, or other documentation Company customarily makes available to customers.

13.2 Audit Limitation

To the extent Applicable Data Protection Law requires audit rights, Customer may, no more than once annually and upon at least thirty (30) days' prior written notice, request an audit of Company's compliance with this DPA, provided that:

(a) the audit is limited in scope to matters reasonably necessary to demonstrate compliance with this DPA;

(b) the audit is conducted during normal business hours;

(c) the audit does not unreasonably interfere with Company's business operations;

(d) the audit does not require access to information concerning other customers, internal source code, trade secrets, privileged materials, or security information that could create a vulnerability;

(e) the audit is conducted by Customer or an independent third-party auditor reasonably acceptable to Company and bound by confidentiality obligations no less protective than those in the Principal Agreement; and

(f) Customer bears all costs of the audit and reimburses Company for its reasonable internal costs incurred in supporting the audit, except where the audit reveals a material breach of this DPA by Company.

13.3 Alternative to On-Site Audit

Company may satisfy audit obligations by providing current third-party audit reports, certifications, penetration-test summaries, security questionnaires, or comparable materials where such materials reasonably demonstrate compliance and make an on-site audit unnecessary.

13.4 Remediation and No Competitive Use

Audit rights shall not be exercised for benchmarking, competitive analysis, vendor comparison, or any purpose unrelated to verifying Company's compliance with this DPA. Customer shall promptly notify Company of any material concerns identified through an audit and provide Company a reasonable opportunity to address them before taking further action, except where prohibited by law.

---

14. CROSS-BORDER TRANSFERS

14.1 General

To the extent Company Processes Customer Personal Data in or transfers Customer Personal Data to a jurisdiction outside the country of origin and such transfer constitutes a Restricted Transfer, the parties agree that the transfer shall be governed by a valid transfer mechanism under Applicable Data Protection Law.

14.2 EEA Transfers

For transfers of Customer Personal Data from the EEA to a country not recognized by the European Commission as providing an adequate level of protection, the SCCs shall apply and are hereby incorporated by reference as follows:

(a) where Customer is Controller and Company is Processor, Module Two (Controller to Processor) of the SCCs shall apply;

(b) where Customer is Processor and Company is Subprocessor, Module Three (Processor to Processor) of the SCCs shall apply;

(c) Clause 7 (Docking Clause) shall apply;

(d) in Clause 9, Option 2 shall apply, and the time period for prior notice of Subprocessor changes shall be as set forth in Section 9 of this DPA;

(e) in Clause 11, the optional language shall not apply unless required by applicable law;

(f) in Clause 17, the governing law shall be the law of Ireland, unless another EU Member State law is required by law;

(g) in Clause 18, disputes shall be resolved before the courts of Ireland, unless another EU Member State court is required by law; and

(h) Annexes I and II to the SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA and the security measures described in this DPA and/or Company's applicable security documentation.

14.3 UK Transfers

For Restricted Transfers of Customer Personal Data from the United Kingdom, the SCCs shall apply as modified by the UK International Data Transfer Addendum, or such other lawful UK transfer mechanism as may replace it from time to time. The tables in the UK addendum shall be deemed completed with the corresponding information in this DPA and the Principal Agreement.

14.4 Swiss Transfers

To the extent applicable, transfers from Switzerland shall be governed by the SCCs with the modifications required by Swiss law.

14.5 Alternative Transfer Mechanisms

If a valid alternative transfer mechanism becomes available under Applicable Data Protection Law, Company may, upon notice to Customer, replace the SCCs or other transfer mechanism with such alternative mechanism.

14.6 Supplementary Measures

To the extent required by Applicable Data Protection Law, Company shall implement supplementary technical, organizational, or contractual measures reasonably appropriate to the transfer context and nature of the Customer Personal Data, taking into account the services provided, the sensitivity of the data, and relevant legal requirements.

---

15. COMPANY AS SERVICE PROVIDER / CONTRACTOR UNDER U.S. STATE LAW

15.1 Processing Restriction

To the extent any applicable U.S. state privacy law imposes obligations on service providers or contractors, Company shall not:

(a) sell or share Customer Personal Data Processed on behalf of Customer;

(b) retain, use, or disclose such Customer Personal Data for any purpose other than the business purposes specified in the Principal Agreement and this DPA, including the

provision of the Platform and related services, or as otherwise permitted by applicable law; or

(c) retain, use, or disclose such Customer Personal Data outside the direct business relationship between Company and Customer except as permitted by applicable law.

15.2 Permitted Uses

Notwithstanding the foregoing, Company may retain, use, or disclose Customer Personal Data as permitted under applicable U.S. state privacy law for a service provider or contractor, including to:

a. detect data security incidents and protect against malicious, deceptive, fraudulent, or illegal activity;

b. preserve the integrity or security of systems;

c. identify and repair errors that impair intended functionality;

d. perform internal use reasonably aligned with Customer's expectations and the direct business relationship;

e. comply with legal obligations; and

f. collect, use, retain, or disclose de-identified or aggregated data in accordance with applicable law.

15.3 No Combination for Independent Profiling

To the extent required by applicable U.S. state privacy law, Company shall not combine Customer Personal Data received from or on behalf of Customer with personal information received from another person or collected from Company's own interactions with an individual, except as permitted by applicable law for a service provider or contractor, including for security, fraud prevention, legal compliance, internal operational uses, and de-identification.

---

16. COMPANY CONTROLLER-SIDE RIGHTS AND RESERVED USES

16.1 Company Controller Processing

Customer acknowledges and agrees that Company may Process certain data as an independent Controller, and not as Processor, including:

a. Business Contact Data for account administration, billing, collections, contract management, renewals, notices, relationship management, and service communications;

b. Usage Data, telemetry, logs, and diagnostic information for service integrity, debugging, capacity planning, feature development, analytics, abuse prevention, and product improvement;

c. Security-related information for identity verification, authentication, fraud prevention, intrusion detection, threat analysis, incident response, and legal defense;

d. information necessary to comply with law, regulation, legal process, or lawful governmental request; and

e. information used to create, train, refine, test, validate, and improve Company's models, analytics, simulation methodologies, and services, provided that Company's use of Personal Data for such purposes complies with Applicable Data Protection Law.

16.2 Derived Data Ownership

As between the parties, Company exclusively owns all right, title, and interest in and to Derived Data. Nothing in this DPA grants Customer any right, title, or interest in Derived Data, Company models, Company methodologies, Company analytics, or Company product improvements.

16.3 De-Identification

Company may de-identify Customer Personal Data and other data in accordance with Applicable Data Protection Law and may use, retain, disclose, commercialize, and otherwise exploit de-identified data and aggregated data for any lawful purpose. Customer agrees that de-identified and aggregated data are not Customer Personal Data and are not subject to deletion, return, portability, or access obligations under this DPA except as required by law.

---

17. LIABILITY

17.1 Liability Allocation

The total aggregate liability of each party and its Affiliates arising out of or relating to this DPA, whether in contract, tort, statute, or otherwise, shall be subject to the exclusions and

limitations of liability set forth in the Principal Agreement, and such limitations shall apply to all claims under this DPA taken together with all claims under the Principal Agreement, unless Applicable Data Protection Law requires otherwise.

17.2 No Expansion

This DPA does not create or increase either party's liability beyond that stated in the Principal Agreement except to the extent such limitation is prohibited by Applicable Data Protection Law.

---

18. TERM AND TERMINATION

18.1 Term

This DPA shall remain in effect for so long as Company Processes Customer Personal Data subject to this DPA.

18.2 Survival

The provisions of this DPA that by their nature are intended to survive termination or expiration shall survive, including, without limitation, provisions relating to confidentiality, liability, deletion and retention exceptions, audits, Controller-side rights, cross-border transfers, and governing law.

---

19. MISCELLANEOUS

19.1 Governing Law

Except as otherwise required by the SCCs or Applicable Data Protection Law with respect to Restricted Transfers, this DPA shall be governed by the governing law specified in the Principal Agreement. If the Principal Agreement does not specify governing law, this DPA shall be governed by the laws of the State of Delaware, without regard to conflict-of-laws principles.

19.2 Severability

If any provision of this DPA is found invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the invalid or unenforceable provision shall be interpreted to preserve, to the maximum extent possible, the parties' original intent.

19.3 Amendment

Company may update this DPA from time to time to reflect changes in Applicable Data Protection Law, guidance, or transfer mechanisms, provided that any such update does not materially reduce the level of protection for Customer Personal Data without notice to Customer. Material updates may be communicated by posting a revised DPA, by email, or through the Platform.

19.4 Entire Agreement

This DPA, together with the Principal Agreement and any incorporated transfer mechanism or schedules, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes prior discussions or agreements relating specifically to that subject matter.

19.5 Counterparts; Electronic Acceptance

This DPA may be executed in counterparts, including by electronic means, click-through acceptance, or incorporation by reference into electronic terms accepted by Customer, each of which shall be deemed an original and together shall constitute one instrument.

SCHEDULE 1

DETAILS OF PROCESSING AND TRANSFERS

This Schedule 1 forms part of the DPA and, where applicable, the SCCs.

A. List of Parties

Data Exporter
The Data Exporter is the Customer entity identified in the Principal Agreement and any of its authorized Affiliates that transfer Customer Personal Data to Company for Processing under the Principal Agreement.

Data Importer
The Data Importer is **Temperpack Technologies Inc.**, a Delaware corporation, with principal offices at 4101 Carolina Avenue, Richmond, Virginia 23222 U.S.A.

B. Description of Transfer

Categories of Data Subjects

May include:

a. Customer personnel and representatives;

b. Customer-authorized users;

c. business contacts included in orders, shipments, support, testing, sample, or account records; and

d. individuals whose Personal Data is submitted to the Platform by or on behalf of Customer.

Categories of Personal Data

May include:

a. names;

b. business contact information;

c. company and account identifiers;

d. job titles and departments;

e. user names and authentication-related data;

f. shipment contact data;

g. support correspondence; and

h. records or reports containing Personal Data to the extent submitted by or on behalf of Customer.

Special Categories of Data

None are intended to be transferred. Customer shall not submit special categories of personal data or other sensitive regulated data unless expressly agreed in writing by Company.

Frequency of Transfer

Continuous, intermittent, or on demand, depending on Customer's use of the Platform.

Nature of Processing

Collection, storage, hosting, retrieval, transmission, display, analysis, support, deletion, and other Processing necessary to provide the Platform and related services.

Purpose of Transfer and Further Processing

To provide the Platform and related contracted services to Customer, including account functionality, business information access, analytics, shipment-related interfaces, simulation support, support services, and operational administration.

Retention

For the term of the Principal Agreement and for any additional period required under Company's retention, backup, legal, compliance, fraud prevention, and security obligations and rights as described in this DPA.

C. Competent Supervisory Authority

The competent Supervisory Authority shall be determined in accordance with the GDPR and the SCCs, and where the SCCs designate a Member State law, the corresponding authority in that Member State shall apply.

D. Technical and Organizational Measures

The technical and organizational measures are those described in Section 7 of this DPA and in Company's then-current security documentation made available to Customer, if any.

SCHEDULE 2

UK ADDENDUM PLACEHOLDER TERMS

To the extent the UK International Data Transfer Addendum applies:

a. the parties agree that the SCCs referenced in this DPA are the Approved EU SCCs;

b. the start date is the effective date of the Principal Agreement or the commencement of the relevant transfer, whichever is earlier;

c. the parties are as identified in Schedule 1;

d. the Appendix Information is set forth in Schedule 1 and this DPA; and

e. neither party may unilaterally amend the approved addendum except as permitted by applicable law or official guidance.

SCHEDULE 3

PROCESSOR / CONTROLLER ROLE ALLOCATION EXAMPLES

This Schedule is interpretive and intended to assist with role allocation.

A. Company as Processor

Company acts as Processor where Customer instructs Company to Process Personal Data solely on Customer's behalf for purposes such as:

i. hosting Customer-uploaded account or contact information in the Platform;

ii. enabling Customer's authorized users to access customer-specific records;

iii. processing Personal Data included in shipment, support, sample, or report records submitted by Customer;

iv. storing and displaying Customer-specific information through Platform interfaces.

B. Company as Independent Controller

Company acts as independent Controller where Company Processes data for its own legitimate business purposes, such as:

i. managing the commercial relationship with Customer;

ii. billing and collections;

iii. account administration and customer communications;

iv. fraud detection, abuse prevention, and security monitoring;

v. legal compliance and response to governmental requests;

vi. internal analytics, service integrity, debugging, and capacity planning;

vii. de-identification, aggregation, benchmarking, and creation of Derived Data;

viii. product and model improvement to the extent permitted by Applicable Data Protection Law.