PRIVACY POLICY

Effective Date: May 6, 2026
Company: Temperpack Technologies Inc., a Delaware corporation, with principal offices at 4101 Carolina Avenue, Richmond, Virginia 23222 U.S.A. ("**Company**," "**we**," "**us**," or "**our**")

This Privacy Policy ("**Policy**") explains how Company collects, uses, discloses, stores, transfers, retains, and otherwise Processes information in connection with Company's web-based digital platform, including all associated modules, dashboards, interfaces, tools, models, analytics, tracking functionality, and related services (collectively, the "**Platform**").

This Policy also explains certain rights and choices that may be available to individuals under applicable law.

---

1. SCOPE AND APPLICATION

1.1 General Scope

This Policy applies to information Processed by Company in connection with:

a. access to and use of the Platform;

b. account creation, account administration, authentication, and support;

c. customer-facing account and order information modules;

d. engineering, simulation, and decision-support tools;

e. tracker-, logger-, and sensor-related interfaces and functionality;

f. communications between Company and Platform users, customers, and prospective customers; and

g. business operations connected to the Platform, including analytics, service integrity, legal compliance, and product improvement.

1.2 Business-to-Business Context

The Platform is designed and operated as a **business-to-business platform**. It is intended for use by businesses and their representatives, employees, agents, and contractors in connection with commercial relationships and operational use cases. It is not intended for personal, household, family, or consumer use.

1.3 Covered Individuals

This Policy may apply to information relating to the following categories of individuals, to the extent their information is Processed in connection with the Platform:

a. customer employees, officers, and representatives;

b. Authorized Users;

c. business contacts;

d. support contacts;

e. shipment-related or operational contacts;

f. testing, reporting, or sample-request contacts;

g. prospective customers or partners interacting with the Platform or related services.

1.4 Territorial Scope

Company may Process information relating to individuals located in the United States, Canada, the United Kingdom, the European Economic Area ("**EEA**"), and other jurisdictions. Company will apply this Policy in conjunction with applicable law, and certain sections specifically address rights or disclosures relevant to certain jurisdictions.

---

2. DEFINITIONS

For purposes of this Policy, the following definitions apply:

2.1 "Affiliate" or "Affiliates"

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

2.2 "Authorized User"

"**Authorized User**" means an individual natural person authorized to access or use the Platform on behalf of a customer, partner, or other business entity.

2.3 "Business Contact Data"

"**Business Contact Data**" means information relating to an individual acting in a business or professional capacity, including name, employer, title, department, business address, business email, business phone number, and similar information.

2.4 “Customer Data”

“**Customer Data**” means business-related information submitted to, stored in, or made available through the Platform by or on behalf of a customer, including account data, order history, SKU information, shipment information, testing and report information, sustainability information, sample records, and similar business records.

2.5 “Derived Data”

“**Derived Data**” means information, models, analytics, benchmarks, aggregated information, de-identified information, trend analyses, performance insights, predictive information, simulation refinements, algorithmic improvements, reports, and other information generated, inferred, transformed, or derived by or on behalf of Company from or through the analysis, combination, transformation, or Processing of data, provided that such information does not identify a particular individual or a particular customer as such.

2.6 “Personal Data”

“**Personal Data**” means information relating to an identified or identifiable natural person, or any similar concept such as “personal information” under applicable law, but excluding data that has been de-identified, anonymized, or aggregated so that it no longer reasonably identifies a natural person.

2.7 “Platform Data”

“**Platform Data**” means information relating to the operation, performance, security, telemetry, diagnostics, usage, maintenance, support, and integrity of the Platform.

2.8 “Process” or “Processing”

“**Process**,” “**Processing**,” **“Processed”**, or similar terms mean any operation or set of operations performed on information, including collection, recording, storage, use, organization, structuring, adaptation, retrieval, consultation, disclosure, transmission, analysis, combination, deletion, destruction, or other handling.

2.9 “Tracker Data”

“**Tracker Data**” means environmental, temporal, or device-related information collected from or through a Tracker or similar monitoring component that interfaces with the Platform, including temperature readings, event timestamps, device identifiers, and similar records.

2.10 “User Data”

"**User Data**" means information entered, uploaded, submitted, transmitted, or otherwise made available to the Platform by or on behalf of a user or customer.

---

3. CATEGORIES OF INFORMATION WE COLLECT

Company may collect, receive, access, generate, or otherwise Process the following categories of information.

3.1 Account and Registration Information

We may collect information necessary to establish, administer, authenticate, and maintain Platform access, including:

a. names;

b. business email addresses;

c. business phone numbers;

d. employer or organization names;

e. titles, roles, or departments;

f. usernames, login identifiers, and account IDs;

g. authentication credentials and related security data; and

h. account preferences and administrative settings.

3.2 Customer Relationship and Commercial Information

We may Process information associated with customer relationships and commercial activity, including:

a. order history;

b. purchase records;

c. account activity;

d. SKU information;

e. pricing information;

f. purchasing patterns;

g. account manager assignments;

h. sample requests and fulfillment records; and

i. customer-specific reports and business records.

3.3 Shipment, Logistics, and Operational Information

We may collect or receive information relating to business operations and shipment activities, including:

a. origin and destination information;

b. shipment timing and route data;

c. shipping-lane information;

d. shipment events and related operational records;

e. payload descriptions;

f. handling assumptions;

g. delivery-related information; and

h. support or escalation records associated with shipment activity.

3.4 Engineering, Simulation, and Decision-Support Inputs

Where users interact with the Platform's engineering, simulation, or decision-support tools, we may collect or receive data such as:

a. payload characteristics;

b. material or product descriptions;

c. packaging preferences and constraints;

d. coolant assumptions;

e. insulation assumptions;

f. duration assumptions;

g. route assumptions;

h. cost inputs or optimization criteria; and

i. operational parameters entered into calculators, solvers, or decision-support tools.

3.5 Testing, Lab, and Sample Information

We may collect or receive information associated with sample, lab, or testing workflows, including:

a. sample history;

b. testing requests;

c. testing records;

d. lab testing history and reports;

e. product or packaging performance records; and

f. notes, attachments, and supporting records associated with such activity.

3.6 Sustainability and Business Intelligence Information

We may collect, calculate, display, or otherwise Process information relating to sustainability, performance, and business metrics, including:

a. sustainability metrics;

b. emissions or equivalent calculations;

c. efficiency measures;

d. account-planning metrics;

e. total-cost-of-ownership or similar calculations;

f. EPR-related calculations or related decision-support information; and

g. business insights, trend information, and general market or technical information.

3.7 Tracker and Sensor Information

If the Platform interfaces with a Tracker or similar monitoring device, we may collect, receive, or display:

a. temperature readings;

b. environmental readings;

c. time-series event data;

d. timestamps;

e. device identifiers;

f. transmission records;

g. monitoring data associated with a shipment, packaging environment, or other operational event.

3.8 Communications and Support Information

We may Process information contained in communications between you and Company, including:

a. emails;

b. support requests;

c. chat records;

d. service tickets;

e. phone call notes;

f. feedback;

g. escalation records;

h. meeting notes;

i. training records; and

j. survey responses.

3.9 Technical, Usage, and Device Information

When the Platform is used, we may automatically collect or generate technical and usage information, including:

a. IP addresses;

b. browser type and version;

c. device type;

d. operating system;

e. session identifiers;

f. access dates and times;

g. clickstream data;

h. page views;

i. feature interactions;

j. referrer URLs;

k. logs, event records, and diagnostic information;

l. crash data and performance metrics; and

m. configuration and telemetry data.

3.10 Cookies and Similar Technologies

We may collect information through cookies, local storage, pixels, tags, SDKs, or similar technologies, including information relating to:

a. authentication and session persistence;

b. security and fraud prevention;

c. user preferences;

d. performance and load balancing;

e. usage analytics; and

f. troubleshooting and support.

3.11 Information from Other Sources

We may receive information from:

a. your organization;

b. other Authorized Users;

c. affiliated entities;

d. service providers;

e. analytics providers;

f. authentication or identity providers;

g. shipping, logistics, or tracking partners;

h. publicly available sources; and

i. third parties that lawfully provide data to us in connection with our business relationship with you or your organization.

---

4. SOURCES OF INFORMATION

We collect information from one or more of the following sources:

4.1 Directly from You

Information you provide through forms, fields, interfaces, uploads, emails, support requests, communications, and Platform interactions.

4.2 From Your Organization

Information provided by the customer organization, account administrators, managers, procurement contacts, lab contacts, or other representatives acting on behalf of a business customer.

4.3 Automatically Through the Platform

Information automatically generated by the Platform or associated systems, including logs, telemetry, usage records, diagnostics, and system interactions.

4.4 From Devices, Sensors, or Trackers

Information captured from Trackers or related monitoring components that interface with the Platform.

4.5 From Third Parties

Information from service providers, analytics partners, cloud providers, security providers, authentication providers, and other vendors or business partners supporting the Platform.

---

5. PURPOSES FOR WHICH WE PROCESS INFORMATION

We Process information for the following business, operational, commercial, legal, and technical purposes:

5.1 To Provide the Platform

We Process information to provide, operate, maintain, and administer the Platform, including to:

a. create and manage Accounts;

b. authenticate users;

c. provide access to features, dashboards, and modules;

d. display customer-specific business information;

e. host and present reports, order information, shipment information, testing records, and related business data; and

f. enable customer access to authorized data and tools.

5.2 To Generate Outputs and Operate Platform Tools

We Process information to generate, display, and support Platform Outputs, recommendations, analytics, and modeled scenarios, including in connection with:

a. packaging suggestions;

b. thermal simulations;

c. coolant or packout tools;

d. shipping-lane or route optimization;

e. account-planning support;

f. cost and sustainability tools;

g. calculator and modeling functions; and

h. tracker-related data displays and reporting.

5.3 To Support Product, Service, and Model Improvement

We Process information to improve our products, services, models, algorithms, methodologies, calculations, business processes, and commercial offerings, including to:

a. develop and refine simulation methodologies;

b. improve Output quality and consistency;

c. test new features and workflows;

d. enhance user experience;

e. troubleshoot problems;

f. improve performance, scalability, and reliability;

g. create new digital tools, calculators, dashboards, and services.

5.4 To Create and Use Derived Data

We Process information to create Derived Data, including aggregated, de-identified, benchmark, analytical, and trend information, for purposes such as:

a. business intelligence;

b. performance analysis;

c. model training and validation;

d. internal reporting;

e. product planning;

f. research and development;

g. commercial strategy;

h. customer and market insights; and

i. lawful commercialization of non-identifying aggregated outputs and learnings.

5.5 To Secure the Platform and Protect Rights

We Process information to secure the Platform and protect Company, users, customers, partners, and third parties, including to:

a. authenticate users;

b. detect suspicious, fraudulent, malicious, unauthorized, or abusive activity;

c. monitor for misuse, data leakage, intrusion attempts, and policy violations;

d. investigate incidents and security threats;

e. preserve system integrity; and

f. enforce our Terms and contractual rights.

5.6 To Communicate

We Process information to communicate with users and customer representatives, including to:

a. respond to requests and inquiries;

b. provide support;

c. send service communications;

d. provide updates;

e. address operational or technical issues;

f. deliver notices required by law or contract; and

g. manage the customer relationship.

5.7 To Manage Commercial Relationships

We Process information to manage business relationships and transactions, including for:

a. account administration;

b. internal recordkeeping;

c. sales and account management;

d. billing and collections;

e. contract administration;

f. renewals and service planning; and

g. business forecasting and operational management.

5.8 To Comply with Legal Obligations and Protect Legal Interests

We Process information to:

a. comply with applicable laws, regulations, legal process, and lawful governmental requests;

b. establish, exercise, or defend legal claims;

c. respond to audits, investigations, and disputes;

d. maintain legally required records; and

e. enforce contractual rights and remedies.

---

6. LEGAL BASES FOR PROCESSING (EEA / UK WHERE APPLICABLE)

To the extent the GDPR, UK GDPR, or similar law applies, we rely on one or more of the following legal bases:

6.1 Performance of a Contract

We Process information where necessary to perform a contract to which the relevant individual or business is a party, or to take steps at the request of the individual or customer before entering into a contract, including to provide access to the Platform and related services.

6.2 Legitimate Interests

We Process information where necessary for our legitimate interests or the legitimate interests of a customer, user, or third party, provided such interests are not overridden by the interests or fundamental rights and freedoms of the individual. These legitimate interests may include:

a. operating and improving the Platform;

b. maintaining security and integrity;

c. understanding product use and performance;

d. supporting users and customers;

e. conducting analytics and internal reporting;

f. developing and improving products, services, tools, and methodologies;

g. protecting legal rights and preventing misuse; and

h. administering business relationships.

6.3 Compliance with Legal Obligations

We Process information where necessary to comply with legal or regulatory obligations.

6.4 Consent

Where required by law, we rely on consent, including for certain cookies or similar technologies, or other Processing activities where consent is legally required and no other lawful basis is appropriate.

6.5 No Obligation to Provide Information

Where you choose not to provide information necessary for certain functionality, we may be unable to provide that functionality, maintain access, or respond to requests.

---

7. HOW WE DISCLOSE INFORMATION

We may disclose information to the categories of recipients described below, subject to applicable law:

7.1 Affiliates

We may disclose information to our Affiliates for purposes consistent with this Policy, including operational, support, security, analytics, legal, compliance, and business administration purposes.

7.2 Service Providers and Contractors

We may disclose information to service providers, contractors, and vendors that assist us with:

a. hosting;

b. cloud infrastructure;

c. storage;

d. analytics;

e. authentication;

f. communications;

g. support;

h. security;

i. maintenance;

j. monitoring;

k. professional services; and

l. administrative and operational functions.

Such parties may Process information on our behalf and subject to contractual restrictions where appropriate.

7.3 Business Partners and Integration Partners

We may disclose information to shipping, monitoring, logistics, data, analytics, device, integration, or business partners where reasonably necessary to provide, support, or improve relevant functionality or business operations, subject to appropriate contractual or operational controls where appropriate.

7.4 Within Customer Organizations

Where the Platform is used on behalf of a business customer, information may be disclosed to administrators, managers, or other representatives of that customer

organization consistent with the nature of the Account, authorization settings, and the customer relationship.

7.5 Professional Advisors

We may disclose information to lawyers, attorneys, legal advisors, auditors, accountants, insurers, consultants, lenders, and other professional advisors where necessary to obtain advice, manage risk, enforce rights, or comply with obligations.

7.6 Governmental, Regulatory, and Legal Recipients

We may disclose information to courts, regulators, law enforcement, governmental authorities, or other parties where we believe disclosure is required or appropriate to:

a. comply with law, legal process, or binding request;

b. protect the rights, property, or safety of Company, our customers, users, partners, or others;

c. investigate or prevent fraud, misuse, or unlawful conduct; and

d. establish, exercise, or defend legal claims.

7.7 Corporate Transactions

We may disclose information in connection with actual or proposed mergers, acquisitions, financings, restructurings, asset sales, reorganizations, bankruptcies, or similar corporate transactions, subject to appropriate confidentiality protections where appropriate.

7.8 De-Identified, Aggregated, and Derived Data

We may disclose, commercialize, publish, or otherwise use de-identified data, aggregated data, and Derived Data for any lawful purpose. Such information is not treated as Personal Data where it no longer reasonably identifies an individual.

---

8. DATA CLASSIFICATION; OWNERSHIP; DERIVED DATA

8.1 Distinction Between Personal Data and Other Information

Not all information Processed through the Platform is Personal Data. Much of the information Processed through the Platform consists of business records, operational information, commercial information, system data, or non-personal information.

8.2 Customer Data vs. Derived Data

Information submitted by or on behalf of customers may include Customer Data. However, Company may use Customer Data, Platform Data, usage patterns, Output information, and related information to generate Derived Data.

8.3 Company Rights in Derived Data

As between Company and any user or customer, Company owns and may retain, use, disclose, commercialize, and otherwise exploit Derived Data, subject to applicable law.

8.4 De-Identification and Aggregation

Company may de-identify and aggregate information and may use, retain, disclose, publish, license, or commercialize such information for any lawful purpose. Company will not attempt to re-identify de-identified data except as permitted by law or necessary to validate de-identification methods, maintain security, or comply with law.

---

9. COOKIES AND SIMILAR TECHNOLOGIES

9.1 Use of Cookies

We may use cookies and similar technologies on the Platform for the following purposes:

a. authentication and session management;

b. maintaining user preferences;

c. enabling core functionality;

d. preventing fraud and abuse;

e. measuring performance;

f. troubleshooting and debugging;

g. understanding feature usage and engagement; and

h. improving the Platform.

9.2 Categories of Cookies

Depending on the Platform configuration, we may use:

a. strictly necessary cookies;

b. functional cookies;

c. performance or analytics cookies; and

d. similar local storage or session technologies.

9.3 Cookie Choices

The Platform is an authenticated, access-controlled business-to-business service. Users access the Platform only after affirmatively accepting Company's Terms and Conditions and this Privacy Policy at account registration. Accordingly, Company's legal basis for cookies and similar technologies used on the Platform is contractual necessity (for strictly necessary and functional cookies required to authenticate users and deliver core Platform functionality) and legitimate interests (for performance and analytics cookies used to maintain Platform security, stability, and quality). The Platform does not use advertising cookies or other tracking technologies that require separate opt-in consent under applicable law. No cookie consent banner is presented within the authenticated Platform environment. Users who wish to manage cookies may do so through their browser or device settings as described in Section 9.4, provided that disabling strictly necessary cookies may impair or prevent access to the Platform.

9.4 Browser and Device Controls

You may also be able to control cookies through your browser or device settings. These controls may not affect all technologies, particularly where certain technologies are necessary for Platform functionality or security.

---

10. INTERNATIONAL TRANSFERS

10.1 Cross-Border Processing

Company operates across jurisdictions and may Process information in the United States and other countries in which Company, its Affiliates, or its service providers operate.

10.2 Transfer Locations

Information may be transferred to, stored in, accessed from, or otherwise Processed in:

a. the United States;

b. Canada;

c. the United Kingdom;

d. the EEA;

e. other jurisdictions in which Company or its service providers maintain operations or systems.

10.3 Transfer Mechanisms

Where required by applicable law, Company will implement an appropriate lawful transfer mechanism for cross-border transfers of Personal Data, which may include:

a. Standard Contractual Clauses;

b. a UK transfer addendum;

c. adequacy decisions;

d. other lawful transfer tools recognized under applicable law.

10.4 Legal Differences Between Jurisdictions

Users acknowledge that data protection and privacy laws may differ between jurisdictions and that governmental authorities in certain jurisdictions may have rights of access that differ from those in the individual's jurisdiction of residence.

---

11. DATA RETENTION

11.1 General Retention Approach

We retain information for as long as reasonably necessary for the purposes described in this Policy, including to:

a. provide and administer the Platform;

b. maintain business records;

c. support security and integrity;

d. comply with legal obligations;

e. resolve disputes;

f. enforce agreements;

g. protect rights and interests; and

h. support audits, investigations, and claims.

11.2 Retention Criteria

Retention periods may vary depending on:

a. the nature of the information;

b. the sensitivity of the information;

c. the reason the information was collected;

d. whether the information is needed for ongoing business operations;

e. legal, tax, accounting, audit, or regulatory requirements;

f. litigation hold or dispute considerations; and

g. technical backup and deletion cycles.

11.3 Examples of Retention

Without committing to a specific universal period unless otherwise required by law or contract, we may retain:

a. Account and access records for the duration of account activity and a reasonable period thereafter;

b. commercial, order, and shipment records for business, accounting, audit, and dispute-resolution purposes;

c. support and communication records for service, training, dispute, quality, and legal purposes;

d. logs, telemetry, diagnostics, and security records for security, troubleshooting, and service integrity purposes; and

e. lab, testing, and report records for operational, legal, and business reference purposes.

11.4 Backup Copies

Information may persist in backup copies, archives, disaster-recovery systems, and similar environments for a period of time after active deletion until such copies are overwritten or deleted in the ordinary course.

11.5 Derived Data and De-Identified Data

Derived Data, aggregated data, and de-identified data may be retained indefinitely and are generally not subject to deletion requests to the extent they no longer constitute Personal Data under applicable law.

11.6 Legal Holds

We may retain information longer where necessary to comply with legal holds, preserve evidence, respond to claims or disputes, or comply with law.

11.7 No Obligation to Return or Delete Upon Termination

Company has no obligation to return, export, or delete information submitted to or generated through the Platform upon termination or expiration of a user's access or upon cessation of the business relationship. Company may continue to retain such information in accordance with this Policy, applicable law, and its legitimate business purposes, including for purposes of security, fraud prevention, legal compliance, model and product improvement, internal analytics, and enforcement of its Terms and Conditions. Information that has been de-identified, aggregated, or incorporated into Derived Data will be retained by Company indefinitely. Users and customer organizations are solely responsible for maintaining independent copies of any data submitted to or accessed through the Platform.

---

12. DATA SECURITY

12.1 General Security Measures

Company implements commercially reasonable technical, physical, administrative, and organizational safeguards designed to protect information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized Processing.

12.2 Examples of Measures

Depending on the nature of the Platform and applicable systems, such safeguards may include:

a. role-based access controls;

b. authentication controls;

c. password and credential management;

d. multifactor authentication where deployed;

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

f. logging and monitoring;

g. change management procedures;

h. network security controls;

i. vendor-management processes;

j. backup and recovery procedures;

k. incident response processes; and

l. physical security measures for relevant facilities or infrastructure under our control.

12.3 No Absolute Security

No method of transmission, storage, or Processing is completely secure, and Company does not guarantee absolute security. Users remain responsible for the security of their own systems, credentials, devices, and networks.

12.4 User Security Responsibilities

Users and customer organizations are responsible for:

a. safeguarding credentials;

b. controlling internal access permissions;

c. ensuring proper use of Accounts;

d. maintaining appropriate device and network security; and

e. notifying us promptly of suspected unauthorized access or misuse.

---

13. AUTOMATED PROCESSING; ANALYTICS; OUTPUTS

13.1 Use of Automated Processing

The Platform may use automated tools, rules, models, analytics, simulations, or algorithmic processes to generate Outputs, insights, recommendations, or calculations.

13.2 No Solely Legal or Similarly Significant Automated Decision

Unless expressly stated otherwise in a separate written agreement, the Platform is not intended to make decisions that produce legal or similarly significant effects on individuals without human review.

13.3 Validation and Decision Responsibility

Users are responsible for independently reviewing and validating Outputs before acting on them. Company does not guarantee that any automated Output is accurate, complete, suitable, or compliant for a particular use case.

---

14. INDIVIDUAL RIGHTS AND CHOICES

To the extent required by applicable law, individuals may have rights regarding their Personal Data.

14.1 Potential Rights

Depending on the jurisdiction and applicable law, these rights may include the right to:

a. request access to Personal Data;

b. request correction of inaccurate Personal Data;

c. request deletion of Personal Data;

d. request restriction of Processing;

e. object to certain Processing;

f. request portability of Personal Data;

g. withdraw consent where Processing is based on consent;

h. lodge a complaint with a supervisory authority or regulator.

14.2 Submission of Requests

Requests may be submitted using the contact details provided in this Policy. We may require sufficient information to verify the identity of the requester and the scope of the request.

14.3 Verification

To protect privacy and security, we may take reasonable steps to verify identity before responding to a request. We may deny or limit a request where we cannot verify identity or where applicable law permits or requires us to do so.

14.4 Limits on Rights

Rights requests may be limited where necessary to:

a. protect the rights, privacy, security, or safety of others;

b. protect Company's confidential information, trade secrets, or proprietary systems;

c. preserve Platform security and integrity;

d. comply with legal obligations;

e. maintain legal claims and defenses;

f. avoid disclosing information relating to other customers, users, or individuals; and

g. preserve information that is not legally subject to the relevant request, such as de-identified or aggregated information, or certain Derived Data.

14.5 Role-Based Limits

Where we Process information on behalf of a customer organization, the customer may be the primary party responsible for responding to certain requests. In such cases, we may direct the requester to the relevant customer organization or coordinate with that customer as appropriate.

14.6 No Discrimination

Where required by applicable law, we will not unlawfully discriminate against an individual for exercising applicable privacy rights.

---

15. U.S. STATE PRIVACY DISCLOSURES

15.1 Applicability

Certain U.S. state privacy laws may grant rights to residents of particular states. To the extent such laws apply and no exemption applies, the disclosures in this Section supplement the remainder of this Policy.

15.2 Categories of Information

In the preceding twelve (12) months, we may have collected the categories of information described in Section 3 of this Policy, including identifiers, business contact information, customer relationship data, shipment and operational data, testing and report information, technical and usage information, communications information, and similar information.

15.3 Purposes

We collect and use such information for the purposes described in Section 5 of this Policy.

15.4 Disclosure

We may disclose the categories of information described in this Policy to the categories of recipients described in Section 7 of this Policy.

15.5 Sale / Sharing

Company does not sell Personal Data for monetary consideration in the ordinary sense. To the extent any applicable law defines "sell" or "share" broadly, Company's practices will be governed by the applicable law, applicable exemptions, and the context of the Platform's B2B nature.

15.6 Sensitive Information

Unless specifically stated otherwise, the Platform is not intended to require or solicit sensitive personal information of the kind that would trigger special treatment under consumer privacy laws. If such data is submitted, its Processing remains subject to applicable law, contract, and operational necessity.

15.7 Authorized Agents

Where required by applicable law, individuals may designate authorized agents to make requests on their behalf, subject to verification and authorization requirements.

15.8 Appeals

Where required by applicable law, individuals whose requests are denied may have a right to appeal. Appeal instructions, if applicable, may be obtained by contacting us using the details below.

---

16. EEA / UK ADDITIONAL DISCLOSURES

16.1 Controller Information

For purposes of applicable EEA and UK data protection law, Company may act as a controller of certain Personal Data processed in connection with Platform administration, security, analytics, support, communications, product improvement, and related purposes described in this Policy.

16.2 Rights

Individuals in the EEA or UK may have the rights described in Section 14, subject to applicable conditions and limitations.

16.3 Complaints

Individuals in the EEA or UK may have the right to lodge a complaint with a supervisory authority in the jurisdiction of their habitual residence, place of work, or place of the alleged infringement.

16.4 Legitimate Interests

Where we rely on legitimate interests, those interests may include operation and improvement of the Platform, prevention of misuse, maintenance of security, support of business relationships, internal analytics, and lawful business administration.

---

17. CHILDREN'S PRIVACY

The Platform is not directed to, and Company does not knowingly collect Personal Data directly from, children under eighteen (18) years of age in connection with the Platform. If we become aware that we have knowingly collected Personal Data from a child in a manner prohibited by law, we will take appropriate steps to address it in accordance with applicable law.

---

18. THIRD-PARTY SITES, SERVICES, AND COMPONENTS

The Platform may contain links to, rely on, interoperate with, or display information from third-party sites, services, devices, software, or components. Company is not responsible for the privacy, security, availability, content, or practices of such third parties. Users should review the privacy policies and terms of those third parties where relevant.

---

19. CHANGES TO THIS POLICY

Company may update this Policy from time to time to reflect changes in law, technology, the Platform, our data practices, or our business operations.

Updated versions will become effective upon posting or upon the later effective date stated in the updated Policy. Where required by law, we will provide additional notice or obtain consent in connection with material changes.

Your continued use of the Platform after an updated Policy becomes effective constitutes acknowledgment of the updated Policy to the extent permitted by law.

---

20. CONTACT INFORMATION

If you have questions about this Policy or wish to submit a request under applicable privacy law, you may contact Company at:

Temperpack Technologies Inc.
4101 Carolina Avenue
Richmond, Virginia 23222 U.S.A.
privacy@temperpack.com

---

21. INTERPRETATION

21.1 Consistency with Other Agreements

This Policy should be read together with the Terms and Conditions of Use and, where applicable, any Data Processing Addendum or other contract between Company and the relevant customer. In the event of a conflict between this Policy and a separate written agreement governing the Processing of Personal Data for a business customer, the separate written agreement may control to the extent of the conflict.

21.2 No Contractual Promise Beyond Applicable Law

This Policy is intended to describe Company's general privacy practices. Except where expressly stated otherwise in a separate contract or where required by law, nothing in this Policy creates contractual rights beyond those required under applicable law.

21.3 De-Identified and Aggregated Information

For the avoidance of doubt, this Policy does not restrict Company's use of de-identified data, aggregated data, or Derived Data to the extent such information is not Personal Data under applicable law.