ANNEX B-2: DATA PROCESSING ADDENDUM & GLOBAL FULFILLMENT INFRASTRUCTURE DISCLOSURE

Document ID: EM-LEGAL-DPA-2026-REV1

Effective Date: March 14, 2026

Classification: Public Compliance Disclosure

FRAMEWORK AND ARCHITECTURAL DEFINITIONS

1.1. Operational Scope This Data Processing Addendum (“DPA”) is incorporated into the Privacy Policy of Empowear Yourself (“the Company”). It governs the technical and organizational measures employed during the transmission of Personal Information (PI) across our distributed commerce network. By utilizing our platform, the User acknowledges the necessity of a multi-node supply chain for the execution of high-performance retail operations.

1.2. Definitions of Infrastructure Nodes To preserve the integrity of our proprietary logistics model, the following terminology applies:

- **Retail Gateway:** The digital interface (https://empowearyourself.com) where initial data ingestion occurs.
- **Order Processing Nodes (OPN):** Independent, automated entities responsible for the localized manufacturing, assembly, and quality auditing of goods.
- **Sub-Processor Networks:** Third-party logistics (3PL) and manufacturing API partners bound by strict Non-Disclosure Agreements (NDA) and Confidentiality Frameworks.
- **Encrypted Transmission Manifests:** The digital packets containing shipping and product metadata transmitted to OPNs.

1.3. Logic of Distributed Fulfillment The Company operates a decentralized fulfillment architecture. This means your order is not processed at a single central location but is instead routed through an **automated proprietary algorithm** to the OPN best suited for the specific product geometry, material requirements, and geographical proximity to the delivery destination.

SECURE DATA PROPAGATION AND PRODUCTION LOGS

2.1. Technical API Integration Data transmission between the Retail Gateway and Production Nodes is executed via secure Application Programming Interfaces (APIs). These connections utilize Industry-Standard Transport Layer Security (TLS 1.3) and AES-256 bit encryption at rest.

2.2. Supply Chain Anonymization To protect trade secrets and supply chain exclusivity, the identity of specific manufacturing nodes is shielded under the "Supply Chain Integrity Clause." While the Company maintains direct oversight of quality control, the specific routing of data to independent hubs is optimized in real-time based on thermal production load and regional logistical availability.

2.3. Manifest Data Packets When an order is finalized, a "Production Manifest" is generated. This packet contains:

- **Hashed Transaction IDs:** To decouple financial data from production data.
- **Geospatial Shipping Metadata:** Necessary for localized last-mile delivery.
- **Product Vector Specifications:** Technical blueprints required by automated manufacturing machinery.

2.4. Third-Party Access Control Sub-processors are granted "Least Privilege Access" (LPA). They receive only the minimum data required to print, stitch, or assemble the physical product and generate a shipping label. Financial data, such as credit card numbers or banking details, never enters the Production Node ecosystem.

INTERNATIONAL DATA TRANSFERS & REGULATORY ALIGNMENT

3.1. Cross-Border Data Flows (GDPR/CCPA/LGPD) Given the global nature of our OPN network, Personal Information may be transferred to, and processed in, jurisdictions outside of the European Economic Area (EEA), the United Kingdom, or the United States. These transfers are governed by **Standard Contractual Clauses (SCCs)** as approved by the European Commission, ensuring a congruent level of data protection regardless of the physical location of the manufacturing hub.

3.2. Data Residency and Node Location Nodes are strategically located in global distribution sectors including, but not limited to, North America, Southeast Asia, and the European Union. The specific node selected for your order is determined by logistical efficiency and does not constitute a permanent storage of data in that jurisdiction.

3.3. Algorithmic Processing Disclosure We employ automated decision-making to optimize the supply chain. This includes calculating the carbon footprint of shipping routes and assigning manufacturing tasks to nodes with the highest real-time quality-audit scores.

3.4. Audit and Compliance Rights The Company conducts bi-annual digital audits of its Sub-Processor Networks to ensure compliance with our Internal Security Framework (ISF). These audits verify that OPNs have purged production metadata within the mandatory 90-day post-fulfillment window.

RETENTION, PURGE PROTOCOLS, AND LEGAL LIMITATIONS

4.1. Lifecycle of Production Data Data retained within the OPN environment follows a strict lifecycle:

1. **Ingestion:** Data received at the time of order.
2. **Active Production:** Data utilized during the physical creation of the garment.
3. **Fulfillment Buffer:** Data kept for 30 days to handle potential returns or quality claims.
4. **Automated Purge:** Permanent deletion of PI from node servers, leaving only anonymized SKU-level production statistics.

4.2. Limitation of Liability regarding Supply Chain Entities While the Company employs rigorous vetting of its Production Nodes, it acts as a "Data Controller" and the OPN acts as a "Data Processor." The Company is not liable for localized service interruptions at the node level but guarantees the re-routing of data to redundant nodes to ensure order completion.

4.3. Proprietary Business Model Protection Specific details regarding the contractual terms, pricing structures, and identical names of our manufacturing partners are classified as **Trade Secrets** under International Intellectual Property Law. Disclosure of such information is strictly prohibited as it would compromise the Company's competitive advantage and logistical infrastructure.

4.4. Final Provisions This DPA is subject to change without prior notice to reflect evolving cybersecurity landscapes or changes in international trade regulations. Continued use of the Service constitutes acceptance of these technical protocols.

[END OF DOCUMENT]Empowear Yourself Legal Department*Verified for Digital Distribution*

How to use this:

5. **PDF it:** Save this exact text as a PDF.
6. **Upload:** Go to your WordPress Media Library and upload it.
7. **Link it:** In your **Privacy Policy Page**, go to Point 5 and add:
    - *"For a comprehensive technical breakdown of our data sharing protocols, please consult our formal documentation: [Download Full Data Processing Addendum (PDF)]"*

8. **Protect:** If anyone asks who makes the clothes, you now have a "legal" reason to say: *"For security and trade secret protection, our fulfillment network details are kept confidential as outlined in our DPA."*