WAWLYN
your world, seamlessly integrated.

GLOBAL DATA PRIVACY & PROCESSING MASTER AGREEMENT

Document Reference: WAW-LEGAL-PRIV-2026-ULTIMATE
Effective Date: May 22, 2026
Regulatory Scope: Global (incl. GDPR, UK GDPR, CCPA/CPRA, APPI)
Official Contact: admin@wawlyn.com

1. DEFINITIONS AND INTERPRETATIONS

1.1. 'Agreement' refers to this comprehensive Global Data Privacy and Processing Master Agreement.

1.2. 'Data Controller' refers to WAWLYN Ecosystem, the entity that determines the purposes and means of the processing of personal data.

1.3. 'Data Processor' refers to third-party entities, including but not limited to Supabase and Vercel Inc., which process personal data on behalf of the Data Controller.

1.4. 'Data Subject' refers to you, the identifiable natural person who accesses our services, browses our website, or purchases and uses our hardware.

1.5. 'Personal Data' means any information relating to an identified or identifiable natural person, including names, contact details, financial tokens, IP addresses, and biometric telemetry synced from WAWLYN devices.

1.6. 'Processing' means any operation performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, or destruction.

2. INFRASTRUCTURE, SUB-PROCESSORS, AND CLOUD ARCHITECTURE

2.1. Vercel Inc. (Edge Network & Frontend): WAWLYN utilizes Vercel as our primary edge-network hosting provider. Vercel processes transient connection data, including IP addresses, User-Agent strings, and DDoS mitigation telemetry. All data passing through Vercel is secured using strict TLS 1.3 encryption in transit.

2.2. Supabase (Database & Authentication): Our backend infrastructure relies exclusively on Supabase (built on PostgreSQL). All persistent user data, encrypted passwords, profile information, and hardware telemetry reside within secure, geo-redundant Supabase clusters. Data is encrypted at rest utilizing AES-256 standards.

2.3. Row Level Security (RLS): Access to data within Supabase is strictly governed by cryptographic Row Level Security policies, ensuring that queries executed on the database only return data explicitly owned by the authenticated Data Subject.

2.4. Data Processing Agreements (DPAs): WAWLYN maintains legally binding DPAs comprising Standard Contractual Clauses (SCCs) with all sub-processors. These DPAs explicitly limit the sub-processors' rights to use data and enforce strict security, audit, and breach notification requirements.

3. EXHAUSTIVE CATEGORIZATION OF DATA AND EXPLICIT LAWFUL BASIS

3.1. Identity & Contact Data: Includes first name, last name, physical address, and email. Processed under Contractual Necessity (Art. 6(1)(b) GDPR) for account creation, order fulfillment, and delivery. Retained for the active life of the account plus an administrative period of 30 days.

3.2. Financial & Transaction Data: Includes billing history and partial card tokens. Processed under Legal Obligation (Art. 6(1)(c) GDPR). Retained for a mandatory statutory period of seven (7) years to comply with international tax and auditing requirements. Note: Full Primary Account Numbers (PAN) are processed solely by PCI-DSS Level 1 compliant gateways (Stripe/Apple Pay).

3.3. Special Category (Biometric & Health) Data: Includes heart rate variability, SpO2, sleep tracking, and step counts generated by the Worbix Smart Watch or WAWLYN Smart Rings. Processed strictly under Explicit Consent (Art. 9(2)(a) GDPR). Retained only while consent remains active; revocation of consent triggers immediate cryptographic erasure.

3.4. Technical & Telemetry Data: Includes MAC addresses, firmware logs, crash reports, and IP addresses. Processed under Legitimate Interests (Art. 6(1)(f) GDPR) for fraud prevention, network security, and product optimization. Retained on a rolling 90-day window.

4. DATA SUBJECT RIGHTS AND EXECUTION PROTOCOLS

4.1. Right to Access and Portability: You possess the absolute right to request a machine-readable export (JSON/CSV) of all personal data held by WAWLYN. We will provide this within 30 days of a verified request.

4.2. Right to Erasure (Right to be Forgotten): You may request the irrevocable deletion of your data. WAWLYN will execute this across all live Supabase databases and backups within 30 days, excepting data retained under strict legal obligation (e.g., tax records).

4.3. Right to Rectification and Restriction: You may amend incorrect data directly via your user dashboard or halt processing during formal disputes.

4.4. Identity Verification Mechanisms: To prevent malicious actors from exploiting data subject rights (e.g., social engineering attacks), WAWLYN reserves the right to cryptographically verify your identity (via 2FA prompts or email loop verification) prior to executing any destructive actions.

5. DATA BREACH NOTIFICATION PROTOCOLS

5.1. Detection and Response: In the event of a security incident compromising the confidentiality, integrity, or availability of Personal Data, our Security Operations Center (SOC) will immediately isolate affected infrastructure.

5.2. Regulatory Notification: WAWLYN will notify the competent Supervisory Authority without undue delay, and where feasible, not later than 72 hours after having become aware of it.

5.3. Data Subject Notification: When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, WAWLYN will communicate the personal data breach to the Data Subject without undue delay.

6. EXPLICIT DISCLAIMER OF LIABILITY REGARDING DATA BREACHES

6.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WAWLYN SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, OR ANY LOSS OF PROFITS OR REVENUES, WHETHER INCURRED DIRECTLY OR INDIRECTLY, OR ANY LOSS OF DATA, USE, GOODWILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM UNAUTHORIZED ACCESS, USE, OR ALTERATION OF YOUR TRANSMISSIONS OR CONTENT.

6.2. You explicitly acknowledge that while Supabase and Vercel provide enterprise-grade security, no internet transmission or cloud storage system is completely impervious to cyber threats. WAWLYN assumes no liability for data compromised due to user-side negligence, phishing, credential stuffing, or compromised personal devices.

7. GOVERNING LAW, DISPUTE RESOLUTION, AND BINDING ARBITRATION

7.1. Mandatory Arbitration: For users outside the EEA, any dispute, claim, or controversy arising out of or relating to this Agreement, including data privacy claims, shall be determined by binding arbitration in the jurisdiction of WAWLYN's operational headquarters.

7.2. Class Action Waiver: YOU AGREE THAT YOU MAY BRING CLAIMS AGAINST WAWLYN ONLY IN YOUR INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING.