WAWLYN
your world, seamlessly integrated.

COMPREHENSIVE WEBSITE & PRODUCT PRIVACY POLICY

Document Reference: WAW-PRIV-2026-WEB-ULTIMATE
Effective Date: May 22, 2026
Regulatory Scope: Global E-Commerce & Hardware Users
Official Contact: admin@wawlyn.com

1. INTRODUCTION AND SCOPE

1.1. Commitment to Privacy: WAWLYN Ecosystem ("WAWLYN", "we", "us", "our") deeply respects your right to privacy. We understand that in the modern era of connected smart devices, the trust you place in us to safeguard your personal, financial, and biometric data is paramount. This Comprehensive Website & Product Privacy Policy (the "Policy") meticulously details how we collect, process, secure, and disseminate your data.

1.2. Scope of Policy: This Policy applies universally to all interactions you have with WAWLYN, including but not limited to visiting our web domains (hosted on Vercel), utilizing our mobile companion applications (iOS and Android), and operating our ecosystem of hardware devices (Wyn Pad, Worbix, Wryny, Wypods, Wynqo).

1.3. Regulatory Alignment: This Policy has been engineered to strictly adhere to the highest global standards of data protection, specifically complying with the General Data Protection Regulation (EU) 2016/679 (GDPR), the UK GDPR, the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CTDPA), the Utah Consumer Privacy Act (UCPA), and the Act on the Protection of Personal Information (APPI) of Japan.

1.4. Changes to the Policy: We may update this Policy from time to time. We will notify you of any material changes by posting the new Privacy Policy on this page and updating the "Effective Date". You are advised to review this Privacy Policy periodically.

2. EXHAUSTIVE CATEGORIZATION OF DATA WE COLLECT

We collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

2.1. Identity Data: Includes first name, last name, maiden name, username or similar identifier, marital status, title, date of birth, and gender.

2.2. Contact Data: Includes billing address, delivery address, email address, and telephone numbers.

2.3. Financial Data: Includes bank account and payment card details. (Note: WAWLYN utilizes tokenized payment gateways; we do not store full Primary Account Numbers (PAN) on our Supabase instances).

2.4. Transaction Data: Includes details about payments to and from you and other details of products and services you have purchased from us.

2.5. Technical Data: Includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, edge-network routing data processed by our Vercel hosting infrastructure, and other technology on the devices you use to access this website.

2.6. Profile Data: Includes your username and password, purchases or orders made by you, your interests, preferences, feedback, and survey responses.

2.7. Usage Data: Includes information about how you use our website, products, and services.

2.8. Marketing and Communications Data: Includes your preferences in receiving marketing from us and our third parties and your communication preferences.

2.9. Special Categories of Personal Data (Biometrics & Health): Our wearable devices (e.g., Worbix Smart Watch, WAWLYN Smart Rings) are equipped with advanced biometric sensors. If you explicitly opt-in, we collect: Heart rate variability (HRV), resting heart rate, blood oxygen saturation (SpO2), electrocardiogram (ECG) approximations, sleep stage tracking (REM, Light, Deep), step count, estimated caloric burn, and female cycle tracking data. We do not collect information about criminal convictions and offences.

3. METHODS OF DATA COLLECTION

3.1. Direct Interactions: You may give us your Identity, Contact, and Financial Data by filling in forms or by corresponding with us by post, phone, email, or otherwise. This includes personal data you provide when you apply for our products, create an account, subscribe to our publications, request marketing, enter a competition, or give us feedback.

3.2. Automated Technologies or Interactions: As you interact with our website and hardware, we will automatically collect Technical Data about your equipment, browsing actions, and patterns. We collect this personal data by using cookies, server logs, web beacons, telemetry agents on our hardware, and other similar technologies.

3.3. Third Parties or Publicly Available Sources: We may receive personal data about you from various third parties and public sources, including analytics providers like Google, advertising networks, search information providers, and technical, payment, and delivery services.

4. HOW WE USE YOUR PERSONAL DATA AND LAWFUL BASIS

We will only use your personal data when the law allows us to. Below is a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so:

4.1. To register you as a new customer: (Lawful basis: Performance of a contract with you).

4.2. To process and deliver your order, including managing payments and collecting money owed to us: (Lawful basis: Performance of a contract, Necessary for our legitimate interests to recover debts due).

4.3. To manage our relationship with you, including notifying you about changes to our terms or privacy policy, and asking you to leave a review or take a survey: (Lawful basis: Performance of a contract, Necessary to comply with a legal obligation, Necessary for our legitimate interests to keep our records updated and study how customers use our products/services).

4.4. To administer and protect our business and this website, including troubleshooting, data analysis, testing, system maintenance, support, reporting, and hosting of data on Vercel/Supabase: (Lawful basis: Necessary for our legitimate interests for running our business, provision of administration and IT services, network security, and to prevent fraud).

4.5. To process your Biometric and Health Data for the purpose of displaying fitness metrics, health trends, and syncing to health aggregation apps: (Lawful basis: Explicit, affirmative consent under GDPR Article 9(2)(a)).

5. DISCLOSURES OF YOUR PERSONAL DATA

We may share your personal data with the parties set out below for the purposes set out in section 4 above.

5.1. Internal Third Parties: Other companies in the WAWLYN Group acting as joint controllers or processors who are based globally and provide IT, logistics, and system administration services.

5.2. External Third Parties: Authorized sub-processors and partners include:

- Supabase (PostgreSQL): Our primary database and authentication infrastructure provider, handling encrypted storage of user profiles and telemetry.
- Vercel Inc.: Our global edge network and frontend deployment platform, handling secure HTTPS request routing.
- Payment Gateways (Stripe, Apple Pay): For processing secure financial transactions.
- Logistics Partners (FedEx, UPS, DHL): For the physical fulfillment, shipping, and delivery of hardware devices.

5.3. Corporate Restructuring: Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

6. INTERNATIONAL TRANSFERS AND SAFEGUARDS

6.1. Cross-Border Data Flow: WAWLYN operates on a global scale. We share your personal data within the WAWLYN Group and with our external third-party infrastructure providers (such as Supabase and Vercel, which operate global server infrastructure). This frequently involves transferring your data outside the European Economic Area (EEA) or the UK.

6.2. Adequacy and Safeguards: Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Adequacy Decisions: We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Standard Contractual Clauses (SCCs): Where we use certain service providers (including cloud hosts in the USA), we utilize specific contracts approved by the European Commission (SCCs, Module 1-4) combined with Transfer Impact Assessments (TIAs) to ensure Schrems II compliance.

7. DATA SECURITY AND INFRASTRUCTURE ARCHITECTURE

7.1. Defense in Depth: We have put in place appropriate technical, organizational, and physical security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorized way, altered, or disclosed.

7.2. Encryption Protocols: All data at rest within our Supabase (PostgreSQL) databases is encrypted using advanced AES-256 algorithms. All data in transit between your browser, our mobile applications, our Vercel edge network, and our databases is encrypted using strict TLS 1.3 cryptographic protocols.

7.3. Row Level Security (RLS) & Access Controls: Our database architecture utilizes advanced Row Level Security, ensuring that database queries can only return data strictly associated with the authenticated user making the request, thereby eliminating horizontal privilege escalation risks. Access to personal data by WAWLYN employees is strictly limited to those employees, agents, contractors, and other third parties who have a business 'need to know'.

7.4. Incident Response and Breach Notification: We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so, typically within 72 hours of becoming aware of the incident.

8. DATA RETENTION POLICY

8.1. Principle of Minimization: We will only retain your personal data for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting, or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

8.2. Statutory Requirements: By law, we have to keep basic information about our customers (including Contact, Identity, Financial, and Transaction Data) for seven (7) years after they cease being customers for international tax and auditing purposes.

8.3. Biometric Erasure: Biometric and Health data is retained only for the active lifecycle of your account. Upon account deletion or explicit revocation of consent, all biometric data is permanently and cryptographically erased from our active Supabase clusters within 30 days, and purged from all encrypted backups within 90 days.

9. YOUR COMPREHENSIVE LEGAL RIGHTS

9.1. Depending on your jurisdiction, you have robust rights under data protection laws in relation to your personal data. These include:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it.
- Object to processing of your personal data where we are relying on a legitimate interest.
- Request restriction of processing of your personal data.
- Request the transfer of your personal data to you or to a third party.
- Withdraw consent at any time where we are relying on consent to process your personal data.

9.2. Exercising Your Rights: To exercise any of these rights, you must contact our Global Data Protection Officer in writing at admin@wawlyn.com. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data.

10. CALIFORNIA AND US STATE-SPECIFIC PRIVACY RIGHTS

10.1. CCPA/CPRA Disclosures: If you are a resident of California, Colorado, Connecticut, Virginia, or Utah, you have specific rights regarding your personal information. We do not "sell" your personal information as traditionally defined. However, our use of targeting cookies may be considered "sharing" under the CPRA.

10.2. Right to Opt-Out: You have the right to direct us not to sell or share your personal information. You can execute this right by clicking the "Do Not Sell or Share My Personal Information" link in our website footer or via the Cookie Consent Banner.

10.3. Non-Discrimination: We will not discriminate against you for exercising any of your CCPA/CPRA rights. We will not deny you goods or services, charge you different prices or rates, or provide you a different level or quality of goods or services.