

PRIVACY POLICY (GDPR COMPLIANT)

WATCHIT PRO B.V.

Effective Date: July 13, 2026

ARTICLE 1: GENERAL PROVISIONS & DATA CONTROLLER

1. **Scope:** This Privacy Policy outlines how WatchIT Pro B.V. (hereinafter: "WatchIT Pro", "we", "us") collects, processes, stores, and transfers Personal Data of natural persons acting as Users, corporate representatives, employees, ultimate beneficial owners (UBOs), or contact persons of corporate entities utilizing our B2B watch auction platform.
2. **Data Controller:** WatchIT Pro B.V., a private limited liability company incorporated under Dutch law, acts as an independent Data Controller as defined under the General Data Protection Regulation (GDPR).
3. **Third-Party Controllers:** Our integrated Payment Provider, Online Payment Platform (OPP), acts as a separate, independent Data Controller concerning financial data, identity verification documents, and compliance records processed under strict Anti-Money Laundering (AML) laws.

ARTICLE 2: CATEGORIES OF PERSONAL DATA PROCESSED

We process the following categories of Personal Data:

- **Identity and Onboarding Data:** Full name, date of birth, nationality, copies of government-issued identification documents (passports/ID cards), and proof of residential address of directors, corporate representatives, and UBOs.
- **Corporate Contact Information:** Corporate email addresses, business telephone numbers, job titles, and physical corporate addresses.
- **Financial and Transactional Logs:** Corporate bank account numbers (IBAN/BIC), payment tracking numbers, billing addresses, transaction history logs, and platform commission history.
- **Technical and Usage Data:** IP addresses, device identifiers, login credentials, browser types, location data via geofencing, API interaction logs, and platform messaging metadata.

ARTICLE 3: LEGAL BASES AND PURPOSES OF PROCESSING

We process Personal Data under the following strict legal frameworks:

1. **Performance of a Contract (Article 6(1)(b) GDPR):** To establish and manage platform accounts, facilitate auctions, automate data matching for DHL logistics, and process communication between Buyers and Sellers.
2. **Compliance with Legal Obligations (Article 6(1)(c) GDPR):** To adhere to mandatory financial reporting, fiscal compliance, corporate record retention, and Anti-Money Laundering (AML) / Know Your Customer (KYC) identity verification directives.
3. **Legitimate Interests (Article 6(1)(f) GDPR):** To safeguard platform security, prevent shill bidding and off-platform circumvention, deploy anti-scraping defenses, analyze marketplace trends, and facilitate corporate restructuring, merges, or asset acquisitions.

ARTICLE 4: DATA TRANSFER IN CORPORATE ACQUISITIONS (M&A CLAUSE)

1. **Unconditional Corporate Asset Transfer:** The User and all associated data subjects explicitly acknowledge, agree, and consent that in the framework of a corporate sale, merger, share transfer, asset buyout, joint venture, or general corporate restructuring of WatchIT Pro B.V., the entirety of the platform's user database—including all historical corporate data, KYC/KYB dossiers, verification logs, transaction histories, platform communications, and associated Personal Data—shall be transferred to the acquiring third-party legal entity as an unencumbered corporate asset.
2. **Legitimate Interest Justification:** This data migration is executed under Article 6(1)(f) GDPR (Legitimate Interest) to preserve operational business continuity, maintain historical marketplace data, defend past transaction records, and facilitate an unhindered transition of platform ownership.
3. **Due Diligence Access:** During the pre-acquisition due diligence phase, redacted or fully audited corporate user data may be made accessible to prospective buyers and their legal/financial advisors under strict Non-Disclosure Agreements (NDAs).
4. **Continuity of Rights:** Following an acquisition, the acquiring entity shall become the new Data Controller and shall remain bound by the data security, processing standards, and usage constraints mandated under the GDPR and this Privacy Policy.

ARTICLE 5: DATA SHARING AND INTERNATIONAL TRANSFERS

1. **Logistics and Payment Integration:** Personal Data is shared via secure API endpoints with our logistics partners (DHL) and financial clearers (OPP) exclusively to execute transactions, generate shipping labels, and manage escrow accounts.
2. **Third-Country Transfers:** If data is transferred outside the European Economic Area (EEA) to an international service provider, such transfers are bound by the European Commission's Standard Contractual Clauses (SCCs) alongside comprehensive technical and organizational security measures to guarantee an equivalent level of data protection.

ARTICLE 6: DATA RETENTION AND DISPOSAL

1. **Standard Retention:** Personal Data processed for account maintenance is retained for the duration of the User's active registration on the Platform.
2. **Statutory Retention:** Following account deactivation, transactional history, financial data, and KYC verification logs are retained for a mandatory period of 7 (seven) years to comply with statutory fiscal, tax, and anti-money laundering legislation under Dutch law.
3. **Data Sanitization:** Upon expiration of the retention periods, data is permanently deleted, or anonymized using industry-standard cryptography to render it impossible to trace back to a natural person.

ARTICLE 7: DATA SUBJECT RIGHTS

Natural persons whose data we process possess the following rights under the GDPR:

- **Right of Access and Portability:** To request a copy of their processed personal data in a structured, machine-readable format.
- **Right to Rectification and Erasure:** To correct inaccuracies or request the deletion of data, provided such data is no longer required for legal compliance or contractual execution.
- **Right to Restriction and Objection:** To object to processing based on legitimate interests or request processing limitations during active disputes.
- **Submission of Claims:** Data subjects may exercise their rights by contacting our Compliance Department. They also possess the statutory right to file an official complaint with the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).