ExeWrap

Privacy Policy (GDPR)

Privacy statement for ExeWrap and the ExeWrap License Server

Document	Privacy Policy (GDPR)
Product	ExeWrap
Provider	Apptimate B.V. (Chamber of Commerce no. 89656202)
Version	1.2
Effective date	26 October 2026

1. Data Controller

Controller	Apptimate B.V.
Address	Postbus 2039, 1990 AA Velserbroek, Nederland
Chamber of Commerce	89656202
Privacy contact	contact@apptimate.nl

Apptimate B.V. processes personal data in accordance with the General Data Protection Regulation (GDPR). This statement explains which data is processed and why.

2. What Data We Process

In connection with license issuance, delivery, renewal matching, and tool downloads, we process the following categories of personal data:

- Name
- Email address
- IP address (including X-Forwarded-For)
- User-Agent
- Product ID
- License ID
- Order / subscription reference
- License type
- Issue and expiration dates
- Feature flags

3. Where Your Data Is Stored

Personal data relating to licensing is stored on the ExeWrap License Server in a storage location that is not publicly accessible. The main stores are:

- License files — contain name and email, together with license identifiers, issue/expiry dates, and features.
- License metadata — contains the email address and download-link information.
- Subscription records — link the payment provider's subscription/order reference to a license, so that renewals can be matched to the correct license.
- Audit logs — one entry per action, containing timestamp, IP address, name, email, license and product identifiers, order reference, license type, and User-Agent.

Separately, our marketing website (exewrap.com) keeps a download log for tool downloads, containing IP address, X-Forwarded-For, and User-Agent.

4. Data We Do NOT Store

- Credit card data
- Other payment data
- Passwords
- Source code
- Your end-customer data

Payments are processed by 2Monetize / 2Checkout. Payment data is processed by that provider; only your name, email, and an order/subscription reference reach us.

5. Purposes and Legal Bases

- License issuance, delivery, and renewal matching — basis: performance of the contract.
- Fraud prevention and handling of chargebacks and disputes — basis: legitimate interest.
- Security, logging, and audit — basis: legitimate interest in the security and integrity of the service.
- Customer communication and support — basis: performance of the contract.
- Website statistics via Google Analytics — basis: consent (see Cookie Policy).

6. Retention Periods

We apply different retention periods per category of data, reflecting how the licensing system actually operates:

- Audit logs (including IP address, email, and User-Agent): retained for up to 180 days, after which the relevant entries are deleted. This period corresponds to the typical chargeback and dispute window. In addition, audit logs are subject to size-based rotation, so older entries may be removed earlier.
- License files and license metadata (including name and email): retained while the license is active and for up to 90 days after the license expires, after which they are deleted. If a

subscription is renewed, this period restarts from the new expiry date so that the license remains available for re-download.

- Subscription records (subscription/order reference linked to a license): retained for as long as necessary to manage and match renewals to the correct license. Because these records are needed to keep renewals linked, they are not subject to the automatic time-based deletion above; they are removed upon a valid erasure request or when no longer needed for renewals.
- Website download log (IP, X-Forwarded-For, User-Agent): retained for up to 180 days, after which the entries are deleted.

Retention is enforced by scheduled deletion routines. Where a configured retention routine is temporarily not active, older data is still bounded by size-based rotation, but exact deletion dates may vary until the routine runs.

7. Recipients and Transfers

We share data only with service providers necessary for our operations, such as the payment provider (2Monetize / 2Checkout) and Google Analytics. Data processing agreements are concluded with processors. Where data is transferred outside the EEA, appropriate safeguards are applied, such as the European Commission’s standard contractual clauses.

8. Data Subject Rights

You have the right of access, rectification, erasure, restriction, objection, and data portability. Requests may be directed to contact@apptimate.nl. On an erasure request, we remove your license file, license metadata, and subscription record, and remove your entries from the audit logs, except where retention is required for fraud prevention or legal compliance, which we weigh per request. You also have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

9. Security

We take appropriate technical and organizational measures to protect personal data. The licensing storage is kept outside the public web root and is not served over the web. Personal-data files and logs are encrypted at rest using AES-256-GCM. This protects against exposure of leaked files, stolen backups, and shared-hosting access; it is not a substitute for protection against a full compromise of the server itself. Access to administrative tooling is restricted and the service is provided over HTTPS. Vulnerabilities may be reported via security@apptimate.nl (see Security & Vulnerability Disclosure Policy).

10. Changes

We may amend this privacy statement. The current version is available at exewrap.com/legal/privacy-policy.pdf.