

Privacy Policy

360 IT CONSULTING, France

Updated 15 October 2026 | Version 2026-10-15

How Houaryou Secure Core handles personal data for website access, supporter downloads, mod licensing and optional support reports.

1. Controller and contact

360 IT CONSULTING, France, operates Houaryou Secure Core at houaryou.com and is the controller for the processing described here. Contact support@houaryou.com for privacy questions or requests.

This notice covers the website and server-side licensing and support services for Houaryou mods, including PropertyManager, CarWizard and protected map packs. External providers also operate their own services under their own privacy notices.

2. Account, Patreon and sign-in data

We store your name, email, Patreon identifier, internal account identifier and licence. Administrators may record an email alias and account-access settings. Patreon synchronization and webhooks supply membership and payment-event status, contribution amounts and history, billing cadence, relationship dates, lifetime support, and trial, gift or follower status when supplied.

These records determine access and support internal administration and supporter reports. This application does not collect card numbers or bank credentials; Patreon and its payment providers handle payments.

Email sign-in uses a single-use link valid for 15 minutes. Login-link requests and successful sign-ins record email, IP address and time. Failed sign-ins can enter technical logs. If you choose Google, Yahoo or Patreon sign-in, the provider handles authentication and returns identity information used to identify your account.

3. Downloads and personalised installers

OIV-route downloads record your account, file identifier and name, generated filename where applicable, whether an OIV was generated, time, IP address and browser user-agent. Administrators can view this history.

Personalised OIV packages contain your licence file and can include your name and email in metadata and your name in the filename. The licence contains encrypted account identifiers, including email and Patreon identity. Keep packages and licences private.

Downloads by accounts marked as top supporters can trigger an administrative email. Internal daily reports can summarize supporter, payment and download activity.

4. Licence checks, HWIDs and restrictions

Licensed clients submit a licence and hardware/device identifier (HWID), with a mod version when supplied. Protected-pack requests also identify the pack, version, game edition and request nonce. We store HWIDs and first discovery dates, and security events including account/email, IP, version, time, result and relevant error context.

An HWID linked to an account is personal data, even if a client hashes it. These records are not anonymous. This notice does not promise a specific client hashing method or a fixed verification frequency.

The standard allowance is three HWIDs unless adjusted for the account. Device limits and account restrictions can automatically block downloads or licence authorization. Shared-IP rules can extend restrictions to accounts sharing an IP with a restricted account. Legitimate shared networks can be affected: contact support for human review, correction or an exception.

Where configured, an on-server GeoIP database estimates country from IP for administrative review. This is approximate IP-based information, not GPS location.

5. Optional diagnostics

The browser debug tool reads eligible text logs from the game folder you select, previews them and sends log text only after submission. Supported clients may also submit reports through the licensed debug API. We store submitted text, log labels, account, time, IP, user-agent and processing status; a notification is emailed to an administrator.

Logs can contain paths, computer/user names, game details, errors or other personal data. Review them and remove unnecessary sensitive information before sending. Reports are optional. The website tool does not upload your entire game folder.

6. Purposes and legal bases

Authentication, entitlement management, downloads, licence verification and requested support use data necessary to perform the service contract or take steps you request before a contract (GDPR Article 6(1)(b)). Security, proportionate abuse prevention, diagnostics and internal service administration rely on legitimate interests in operating and protecting the service (Article 6(1)(f)), subject to a balancing assessment and your rights. Specific legal obligations rely on Article 6(1)(c).

Optional YouTube embedding relies on consent. Refusing videos does not affect sign-in, download or licence entitlement. This notice is information, not blanket consent. Necessary account, entitlement and device/licence data are required to provide the corresponding service.

7. Cookies and external browser requests

Session cookies support sign-in and authentication flows. Form protection may use temporary CSRF cookies. These essential functions are separate from optional video consent. No advertising or audience-measurement integration is configured by this application.

Fonts and interface resources are requested from Google Fonts, jsDelivr and cdnjs; those providers receive connection data such as your IP address. These requests are not controlled by the YouTube choice.

YouTube players stay blocked until you allow them. If allowed, a youtube-nocookie.com player loads and Google/YouTube receives connection and viewing information and may use storage or trackers. The privacy-enhanced domain does not remove the need for your choice. See <https://policies.google.com/privacy>.

We remember your allow/refuse choice locally in this browser for up to six months. Use Cookie settings in the footer or Disable YouTube beside a player to withdraw. Withdrawal removes embedded players and prevents further embedding, but cannot erase data already received by Google or cookies on its domains. Those can be cleared through your browser.

8. Recipients and international processing

Authorized administrators can access records, including through an account-impersonation feature for support and account checks. Hosting, database and email-delivery providers process information necessary to operate the service. Administrative emails can include supporter identity and activity summaries.

Patreon supplies supporter data; chosen sign-in providers handle authentication. External resource providers and YouTube receive browser requests as described above. We do not sell personal data or configure advertising profiles in this application. Disclosure can also occur when legally required or necessary for a specific legal claim.

External providers may process data outside the European Economic Area under their own privacy notices. Hosting/mail-provider identities, processing locations and applicable transfer arrangements must be checked for the deployed service; request details at support@houaryou.com. This notice does not assert that all processing remains in France or that a specific transfer safeguard has been verified.

9. Retention

The database cleanup limits are: login, licence/security and application-error records: six calendar months from the event; download records: twelve calendar months from download; processed debug reports and text: 90 days after being marked processed; unprocessed debug reports: twelve calendar months from submission. A daily server task runs the cleanup after deployment; monitoring that task is required to enforce the limits.

Account, licence, HWID and Patreon-entitlement records are maintained while necessary to provide and verify access, including former-supporter access. They are not removed with routine event logs. Cancelling Patreon does not automatically erase them. Contact us for review or erasure when that relationship has ended. Inactive accounts require a separate review rather than indiscriminate deletion that would remove existing access.

Specific legal obligations or disputes can require a separate restricted archive for the applicable period. Infrastructure logs, administrative email copies, temporary installer files and backups require separate controls with the relevant provider or administrator. Database cleanup does not erase those copies; contact us about the systems relevant to your request.

10. Your rights and human review

Subject to applicable conditions, you may request access, correction, erasure, restriction or portability, and object to legitimate-interest processing. You can withdraw optional video consent at any time. Erasure can affect services requiring an account/licence, and lawful retention exceptions may apply.

Write to support@houaryou.com, preferably from your account email. We may request proportionate identity verification. We normally respond within one month; a lawful extension will be explained within that period. You can complain to the CNIL at <https://www.cnil.fr/fr/plaintes> or another competent supervisory authority.

Membership, device-limit and shared-IP decisions can be automatic. Ask for human review, explain your situation and request correction. Whether a decision falls under GDPR Article 22 depends on its effects; this notice does not remove any applicable rights.

11. Security and changes

Authentication, access controls and licensing protections restrict access to account and protected-pack information. They do not make account-linked data anonymous or guarantee absolute security.

This version replaces earlier claims that no personal data or history was stored. Future material processing changes will be reflected in this notice. Processing requiring consent needs its own valid choice.