

COOKIE POLICY

Effective Date: 05.07.2026 | Last Updated: 05.07.2026 | Version: 1.0

This Policy explains cookies, local storage, session storage, SDKs and similar technologies used or potentially used through the Lootory Telegram Mini App and official websites.

CURRENT STATUS AS OF 05.07.2026

No optional analytics, behavioural advertising or marketing technology is represented as active unless it appears in the live in-product Technology Inventory. Exact cookie and storage names must be taken from the production deployment, not invented in this Policy.

1. SCOPE AND CONTROLLER

For technologies deployed and controlled by Lootory, the controller is SIA "Lootory", registration number 40203717544, registered office Irbenes iela 14-83, Riga, LV-1058, Latvia. Privacy questions may be sent to privacy@lootory.gg.

This Policy applies to lootory.online, the Lootory Telegram Mini App and, after formal launch, lootory.gg. Telegram, Wallet providers, payment Providers and other third parties may independently control their own technologies.

2. WHAT STORAGE TECHNOLOGIES ARE

Technology	Description
Cookies	Small files that a browser or embedded WebView may store and return to a service.
Local storage	Browser or WebView storage that usually remains until deleted, overwritten or expired.
Session storage	Storage that usually remains only for the active browser or Mini App session.
IndexedDB or cache storage	Structured or cached data stored in the browser or WebView.
SDKs and embedded scripts	Software components used for functions such as Wallet connection, security, errors, support, analytics or payments.
Pixels, tags and identifiers	Technologies that may record events, attribution, device or session information.

3. LEGAL APPROACH

Storing information on or accessing information from a user's device generally requires clear information and prior consent unless the technology is strictly necessary to provide a service expressly requested by the user or another legal exemption applies.

Where consent is required, it must be freely given, specific, informed, unambiguous, active and withdrawable. Lootory will not infer consent from opening the Mini App, scrolling, closing a banner, accepting the Terms or continuing to use the Platform.

4. CURRENT DEPLOYMENT STATUS

Category	Current status	Consent position
Strictly necessary	May be active where required for session continuity, security, authentication, requested Wallet connection, consent preferences or Transaction continuity.	No consent where a legal exemption applies; information is still provided.
Optional functional	Not represented as active unless shown in the live Technology Inventory.	Prior consent where required.
Analytics and performance	Not represented as active unless shown in the live Technology Inventory.	Prior consent where required.
Marketing and advertising	No behavioural advertising or retargeting is represented as active at publication.	Prior consent required where applicable.
Provider technologies	May activate only when the user enters a Wallet, payment, verification or other third-party flow.	Depends on necessity, Provider role and applicable law.

5. STRICTLY NECESSARY TECHNOLOGIES

Strictly necessary technologies may support:

- session continuity and routing;
- Telegram Mini App operation and authentication state;
- Account and transaction security;
- prevention of duplicate or conflicting submissions;
- consent-preference storage;
- requested language or accessibility settings;
- Wallet connection initiated by the user;
- Transaction-stage continuity and fraud prevention.

A technology is not strictly necessary merely because it improves analytics, advertising, engagement or internal reporting. Data obtained through a necessary technology must not be repurposed for optional tracking without an appropriate basis and consent where required.

6. OPTIONAL FUNCTIONAL TECHNOLOGIES

Optional functional technologies may remember non-essential preferences, enable optional support widgets, display third-party media or provide other convenience features. Where consent is required, they remain disabled until actively enabled.

Refusing optional functional technologies does not prevent access to core functionality that does not depend on them, although the specific optional feature may be unavailable.

7. ANALYTICS AND PERFORMANCE

If introduced, analytics may measure screens, feature adoption, navigation, errors, performance and aggregated engagement. Optional analytics must remain disabled until valid consent where required.

Analytics should avoid private Transaction messages, evidence, credentials, unnecessary Wallet data and full IP addresses where a less intrusive configuration is reasonably available.

8. MARKETING AND ADVERTISING

Marketing, retargeting, behavioural advertising and cross-service tracking are not active merely because this category is described. Prior valid consent is required where applicable.

Private Transaction information, dispute evidence, sanctions records, precise Wallet balances and protected or sensitive characteristics must not be used for advertising targeting.

9. SECURITY AND FRAUD-PREVENTION TECHNOLOGIES

Security technologies may protect Accounts, detect malicious requests, prevent automated abuse, identify suspicious changes, protect Wallet-address integrity and prevent duplicate settlement instructions.

A security label does not automatically exempt a technology from consent. Lootory must assess necessity, information accessed, duration, alternatives, reuse and whether a Provider creates an independent profile. Persistent fingerprinting is not introduced by default.

10. TELEGRAM MINI APP ENVIRONMENT

The Lootory Mini App operates in a Telegram-provided environment and embedded WebView. Storage behaviour may be affected by Telegram, the operating system, browser engine, device settings, cache rules and software updates.

Telegram may independently process data or operate technologies under its own terms. The live Technology Inventory should distinguish Lootory-controlled technologies from Telegram-controlled components.

11. WALLET AND PROVIDER TECHNOLOGIES

A Wallet connection may store the selected Wallet provider, public Wallet Address, network, session identifier, connection request or disconnection state only as necessary for the requested function and address integrity.

Lootory-controlled storage must not contain Wallet private keys, seed phrases, recovery phrases or Wallet passwords.

Future payment, conversion, payout or verification Providers may use their own technologies for sessions, fraud prevention, verification, payment and compliance. Their privacy and cookie information applies to independent processing.

12. REFERRAL ATTRIBUTION

A referral link parameter or limited storage may associate a referral with Account creation and qualification. It must be used only for referral attribution, fraud prevention, reward calculation and complaint handling and must not create an unrelated advertising profile.

Device-side referral data should expire when no longer needed. Server-side referral records are retained under the Privacy Policy.

13. CONSENT INTERFACE

Before optional technologies activate, the interface should provide a concise explanation and clear Accept, Reject and Settings choices. Accept and Reject should be comparably accessible and optional categories should not be preselected.

Users should be able to accept all, reject all or choose categories. Optional scripts, SDKs or tags must not transmit data before the required choice.

14. WITHDRAWAL AND PREFERENCE RECORDS

Users must be able to withdraw consent as easily as it was given through a persistent control such as Privacy Settings, Cookie Settings or Storage Preferences.

After withdrawal, optional collection covered by that consent must stop. Lootory may retain a limited record of consent status, categories, policy version, date and withdrawal for the processing period and usually up to three years afterward for accountability.

15. CLEARING STORAGE

Clearing cookies or local storage may sign the user out, disconnect a Wallet interface, remove preferences, interrupt an unfinished form or require re-authentication.

Clearing device storage does not cancel a funded Transaction, refund Escrowed Funds, reverse blockchain activity, change the 2-of-3 threshold, remove contractual obligations or erase public TON records.

16. THIRD-PARTY CONTENT AND INTERNATIONAL TRANSFERS

Optional embedded content should remain inactive until the required choice. After activation, a third party may process information independently under its own privacy notice.

Where a Storage Technology transfers personal data outside the EEA, Lootory must assess the recipient, destination, purpose, safeguards, sub-processors, retention and necessity under the Privacy Policy.

17. LIVE TECHNOLOGY INVENTORY

Before production publication and after each material deployment change, Lootory must scan the live Mini App and websites and maintain a public inventory containing the exact information below.

Field	Required information
Name	Exact cookie, local storage key, SDK, script or identifier name.
Provider and role	Lootory or third-party Provider; processor or independent controller where known.
Category and purpose	Strictly necessary, functional, analytics, marketing or Provider-specific purpose.
Data	Information stored, read or transmitted.
Duration	Session, exact expiry, until deletion or another precise criterion.
Consent	Whether prior consent is required and the reason.
Recipients and location	Who receives the data and relevant processing countries.
Control	How the user withdraws or clears the technology.
Review date	Date the inventory item was last technically verified.

NO SPECULATIVE INVENTORY

Lootory must not publish invented cookie names, durations or Provider details. If no optional technology in a category is active, the inventory should state: "No technologies in this optional category are currently active."

18. USER RIGHTS AND COMPLAINTS

Where information associated with Storage Technologies is personal data, users may have rights of access, rectification, erasure, restriction, objection, portability and withdrawal of consent under the Privacy Policy.

Requests may be sent to privacy@lootory.gg. Users may also complain to the Latvian Data State Inspectorate or another competent supervisory authority.

19. CHANGES

Lootory may update this Policy because of new features, new technologies, Provider changes, Telegram or WebView changes, legal developments, security requirements or correction of errors.

A materially new optional purpose requires a new valid choice where required. Continued use is not consent to new optional tracking.

CONTACT AND OPERATOR

Purpose	Contact
General and Transaction support	support@lootory.gg
Privacy and data-protection matters	privacy@lootory.gg
Security incidents and vulnerability reports	security@lootory.gg
Formal legal and intellectual-property notices	legal@lootory.gg

Operator: SIA "Lootory", registration number 40203717544, registered office Irbenes iela 14-83, Riga, LV-1058, Latvia.