

Toffee Wallet Privacy Policy

Last Updated: November 3rd, 2025

Please review this Privacy Policy regularly, as it may be updated from time to time. Any changes will be effective immediately upon posting on our website or app.

1. Overview

Galactica Games Inc. dba **Toffee Wallet** (the “Company”) respects your privacy and is committed to protecting personal and nonpublic personal information, in accordance with relevant privacy laws. This Policy explains how information is collected, used, shared, and safeguarded.

The Company complies with applicable privacy and data protection laws in the jurisdictions where we operate. These include, where relevant:

- The European Union General Data Protection Regulation (EU GDPR) and the UK GDPR/Data Protection Act 2018;
- The Gramm-Leach-Bliley Act (GLBA), the Right to Financial Privacy Act (RFPA), the Children’s Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA), and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) in the United States;
- The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; and
- Other applicable regional and national privacy laws.

This Policy is designed to reflect the highest standards of global privacy regulation, including principles of fairness, transparency, purpose limitation, data minimization, security, and individual rights. Depending on your location, you may have specific legal rights regarding your personal information, which are outlined below.

2. CAN-SPAM Policy Requirements

The Company complies with all CAN-SPAM requirements when sending commercial email. This includes:

- using accurate “From”, “To”, and routing information.
- Ensuring subject lines are not deceptive or misleading.
- Clearly identifying commercial email as an advertisement or promotion.
- Including a valid physical address.
- Providing clear and easy opt-out instructions in every message, which are honored within 10 business days.
- Prohibiting the transfer of opt-out recipient email addresses, except to ensure CAN-SPAM compliance.

3. GLBA Privacy Policies (if applicable)

The Company complies with the Gramm-Leach-Bliley Act (GLBA) Privacy Rules, which require financial institutions to safeguard consumer information and provide privacy notices.

Information Sharing

We may share customer information with affiliates, service providers and payment processors to carry out daily operations (such as, ID verification, transaction processing, reward facilitation, etc.). We may also share information when required by law.

Opt-Out Rights

Customers will be given opt-out opportunities where required, such as when sharing beyond operational business needs or with affiliates for marketing.

Notices to Consumers

GLBA privacy notices are provided when a customer relationship is established and annually thereafter, outlining categories of information collected, disclosed, and customer rights.

Restrictions

The Company will not disclose account numbers or similar identifiers to non-affiliated third parties for marketing purposes.

4. RFPA Policy Requirements

The Company complies with the Right to Financial Privacy Act (RFPA). Federal authorities may only access customer financial information with:

- a valid subpoena, warrant, or customer consent, or
- Other exceptions permitted by law.

We may be required by court order to delay notifying a customer for up to 90 days if disclosure would jeopardize an investigation.

5. COPPA Policy Requirements

The Company does not knowingly collect data from children under 13. If services are ever directed to children under 13, we will comply with COPPA by:

- Posting clear privacy notices.
- Obtaining verifiable parental consent before collecting data.
- Allowing parents to review or delete their child's information.
- Limiting data collection to what is reasonably necessary for participation.
- Implementing strict security safeguards for children's data.

6. Your Privacy Rights

Depending on where you live, you may have certain legal rights with respect to your personal information. The Company respects and honors these rights where applicable. They may include:

- **Right of Access:** To request a copy of the personal information we hold about you.
- **Right of Correction/Rectification:** To correct inaccurate or incomplete personal information.
- **Right of Erasure** (“Right to be Forgotten”): To request deletion of your personal information, subject to legal exceptions.
- **Right to Restrict Processing:** To request that we limit how we use your personal information.
- **Right to Data Portability:** To request that we transfer your information to another service provider in a structured, commonly used format.
- **Right to Object:** To object to processing of your personal information in certain circumstances, including direct marketing.
- **Right to Withdraw Consent:** Where processing is based on consent, you may withdraw it at any time.
- **Right to Limit Use of Sensitive Data:** In some jurisdictions, you may limit how sensitive information is used.
- **Right to Opt-Out of Sale or Sharing:** In jurisdictions such as California, you may opt-out of the sale or sharing of your personal information.
- **Right to Non-Discrimination:** You will not be discriminated against for exercising your privacy rights.

6.1 How to Exercise Your Rights

We provide clear instructions and, where required, online portals to help you exercise your rights. Requests will be subject to verification to protect your identity. We will respond within the timelines required by law.

Local Rights

You may have additional rights depending on the laws of your country or region. We will comply with such rights to the extent required by applicable law.

These rights may not be absolute and can be subject to limitations under applicable law.

7. Purpose of Data Collection and Use

We collect and use a range of personal, financial, technical, and behavioural data to operate, improve, and personalize the Toffee Wallet experience and the broader Galactica Games ecosystem. Our legal bases for processing personal data include the performance

of a contract, compliance with legal obligations, legitimate interests in operating and improving our services, and, where required, your consent.

The categories of data and how we use them are set out below:

7.1 Account and Identity Data

What we collect:

- Name, username, email address, phone number, date of birth, country of residence, and government-issued identification (for KYC/verification).

Why we use it:

- To create and manage your Wallet account.
- To verify your identity and comply with Know Your Customer (KYC), Anti-Money Laundering (AML), and Counter-Terrorist Financing (CFT) laws.
- To communicate with you about your account, security updates, and policy changes.

7.2 Financial and Transaction Data

What we collect:

- Wallet balances, transaction amounts, purchase history, load and redemption records, linked payment instrument tokens, and reward program data.

Why we use it:

- To process payments, apply rewards, and maintain transaction histories.
- To detect, investigate, and prevent fraud or unauthorized activity.
- To support accounting, auditing, and tax reporting obligations.
- To identify spending patterns that inform our recommendation engine and promotional offers.

7.3 Gameplay and Behavioural Data

What we collect:

- Game participation metrics, time spent in games, in-app actions, achievements, reward redemptions, engagement with offers, and clickstream data from in-app browsing.

Why we use it:

- To understand how players interact with games and commerce features.
- To personalize gameplay recommendations, promotions, and in-app content.
- To create behavioural profiles that improve user experience and optimize marketing relevance.

- To analyze aggregated trends that guide product design and cross-platform integration strategy.

7.4 Device, Technical, and Usage Data

What we collect:

- Device identifiers (e.g., IP address, advertising ID, operating system, browser type, and version), log files, cookies, and app usage metrics.

Why we use it:

- To maintain the security and performance of the Wallet and associated apps.
- To detect anomalies, prevent fraud, and safeguard transactions.
- To perform analytics and measure performance across platforms and markets.
- To improve compatibility, speed, and reliability of our systems.

7.5 Marketing, Preference, and Communication Data

What we collect:

- Marketing opt-ins, communication preferences, interaction history (emails, notifications, or in-app messages), and response tracking.

Why we use it:

- To manage subscriptions and comply with marketing consent requirements.
- To send promotional messages, rewards, or offers related to games, in-app purchases, and partner products that may interest you.
- To measure campaign performance and refine audience targeting.

7.6 Analytical, Aggregated, and Derived Data

What we collect:

- Insights derived from combining and analysing the above data sets, often pseudonymized or aggregated.

Why we use it:

- To develop new features, scoring models, and prediction systems for user engagement and retention.
- To improve fraud detection, credit risk modelling, and reward optimization.
- To generate anonymized insights for commercial strategy, compliance analytics, and partnership reporting.

7.7 Regulatory and Legal Data

What we collect:

- Records of customer identification, verification logs, regulatory correspondence, and data required for compliance audits.

Why we use it:

- To meet our obligations under the Bank Secrecy Act (BSA), AML/CFT programs, GLBA Safeguards Rule, and related laws.
- To retain legally mandated records and cooperate with lawful investigations.
- To defend or enforce legal claims or compliance obligations.

7.8 Data Used for Personalization and “GCommerce”

What we collect:

- Combined in-game behavior, wallet activity, and marketplace interactions.

Why we use it:

- To present relevant game titles, digital goods, and real-world offers based on your preferences and usage patterns.
- To bridge in-game and out-of-game commerce (“GCommerce”), allowing you to earn, redeem, or spend rewards seamlessly across games and partner merchants.
- To deliver dynamic recommendations that enhance engagement and conversion.

We do not sell personal information for monetary consideration.

Data used for analytics, personalization, or marketing is handled under strict data processing and confidentiality agreements with our trusted service providers.

We use aggregated or pseudonymized data whenever possible to limit the use of directly identifiable information.

8. Information Use & Sharing

For details on the categories of personal information we process, the types of service providers we use, and our use of automated decision-making and AI systems, please see Annex A of this Privacy Policy.

The Company may share information only in the following circumstances:

- With affiliates or service providers to deliver services.
- To process payments, verify transactions or facilitate rewards programs.
- To detect, prevent, or investigate fraud, unauthorized transactions or to resolve disputes.

- When required by law, regulations, or judicial process.
- With government or regulatory authorities for compliance reasons.
- To comply with legal and regulatory obligations under the Bank Secrecy Act, Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) rules, tax reporting laws, and other financial regulations applicable to prepaid access and wallet programs.

We do not disclose account numbers or similar sensitive identifiers to non-affiliated entities for marketing. We do not sell or rent personal information. Any sharing of customer data is limited to service providers under contractual confidentiality and data protection obligations.

9. Data Security & Confidentiality

The Company safeguards all customer information through secure systems, encryption, and strict access protocols. We regularly review our information security controls and incident response procedures to ensure resilience against unauthorized access or misuse.

Toffee Wallet stores all customer data on Google Cloud Platform (“GCP”) infrastructure located in the United States. GCP acts as a data processor under a written data processing agreement that ensures compliance with applicable privacy and security standards, including encryption at rest and in transit.

- Employee access to personal information is limited to those with a business need.
- Employees are trained annually on confidentiality obligations.
- Violations of privacy or security requirements may result in disciplinary action, up to and including termination.

10. International Transfers

For users located outside the United States, we may transfer your personal information to our U.S. operations or to service providers in other countries. Where required by law, such transfers are governed by appropriate safeguards, including the European Commission’s Standard Contractual Clauses and equivalent UK mechanisms.

11. Record Retention

The Company retains data and records related to privacy and marketing in compliance with applicable laws.

- For example, the CCPA requires us to maintain records of consumer requests and our responses for at least two years, and GDPR requires documentation of processing activities.
- Marketing and advertising records are retained as required under applicable law.

Retention periods vary depending on the type of data and the purpose for which it is collected. We apply retention schedules consistent with legal, regulatory, and operational requirements.

12.Data Brokerage Statement

Toffee Wallet is not a “data broker” as defined under applicable U.S. state laws, including the California Civil Code §1798.99.80(d) (as amended by the Delete Act), Vermont Statutes 9 V.S.A. §2430(4), and similar laws in other jurisdictions.

We do not sell, license, or rent personal information about individuals with whom we do not have a direct relationship. All data that we collect is obtained directly from users of Toffee Wallet or through their interactions within the Galactica Games ecosystem.

We use this data to deliver, personalize, and improve the Wallet experience, including analytics, recommendations, and offers relevant to our users’ gameplay and commerce preferences.

Any third parties that process data on our behalf—such as payment processors, analytics vendors, or marketing technology providers—do so under written data processing agreements that limit their use of personal information solely to performing services for Toffee Wallet and prohibit resale or independent use.

If Toffee Wallet ever engages in data activities that would meet the legal definition of a “data broker,” we will comply with all registration, disclosure, and opt-out requirements under applicable law and update this Privacy Policy accordingly.

13.Contact & Governing Law

You may contact our Data Protection Officer with any questions or concerns at support@toffeewallet.com, with the subject line “Attn: Data Protection Officer”.

This Privacy Policy and any related disputes are governed by the same law and jurisdiction as specified in our Terms of Use.

14.Monitoring, Training & Updates

- **Monitoring:**
 - The Company conducts annual independent reviews to ensure privacy compliance.
- **Training:**
 - All employees complete Privacy training each year.
- **Policy Updates:**
 - This Policy is reviewed and updated periodically to reflect changes in applicable global privacy laws. Updates will be posted with a revised “Last Updated” date, and customers are encouraged to regularly review this Privacy Policy.

Annex A – Data Categories, Service Providers & Automated Decision-Making

1. Categories of Personal Information We Process

We may collect and process the following categories of information in connection with your Toffee Wallet account and related services:

- **Identifiers:** such as your name, username, email address, telephone number, date of birth, and government-issued identification numbers (e.g., for identity verification).
- **Financial Information:** including wallet balance, payment card identifiers (tokenized), transaction history, load and redemption records, and reward program data.
- **Device and Technical Data:** such as IP address, device ID, operating system, browser type, and log data generated when you access our app or website.
- **Communications Data:** records of messages or correspondence with us, including customer support interactions.
- **Marketing and Preference Data:** opt-in/opt-out choices, rewards preferences, and participation in promotional or referral programs.
- **Compliance and Risk Data:** information used for fraud detection, sanctions screening, anti-money laundering (“AML”) and Know Your Customer (“KYC”) processes.

These categories correspond to the types of information described in applicable privacy laws, including the CCPA, GDPR, and GLBA, where relevant.

2. Third-Party Service Providers (“TPSPs”)

Toffee Wallet uses trusted third-party service providers to operate and deliver the services you use. These include payment processors, cloud infrastructure partners, identity verification vendors, analytics providers, and compliance technology providers.

Each service provider is contractually required to handle personal information only for the purpose of delivering its specific service to us and in accordance with strict data protection and confidentiality obligations.

If you would like to obtain a current list of categories of third-party service providers used by Toffee Wallet, you may contact our support team at support@toffeewallet.com.

3. Automated Decision-Making and Use of AI

We use automated systems, including algorithms and artificial intelligence (“AI”), to help detect and prevent fraud, verify identity, and assess transaction risk. These systems operate within defined parameters and are monitored by our compliance team to ensure fairness, accuracy, and consistency with applicable law.

Some of our third-party service providers may also use AI or machine-learning models to support fraud prevention, KYC verification, and security monitoring.

We do not use automated decision-making to deny you access to services without human review. Any decision with significant effect on your rights or access to the Wallet is subject to manual verification by a qualified compliance reviewer.

4. Your Rights in Relation to Automated Processing

You may contact us to request further information about how automated decision-making or AI systems are used in connection with your account. Where required by law, you may also object to certain forms of automated processing or request human review of decisions that affect you.