

PRIVACY POLICY

What we see, what we don't, and why that is almost nothing.

DOCUMENT

Privacy Policy

LAST UPDATED

July 2026

APPLIES TO

The Ticket4Life Interface & Protocol on Base

CONTACT

X @Ticket4Life · Telegram

How Ticket4Life handles data: by holding almost none of it.

Plain-language summary: Your wallet address is the only identifier we work with, and it stays pseudonymous. We do not ask for your name, email, phone number, or any identity documents, and we run no KYC. A country-level geo-check happens in memory when the app loads and is never stored. Analytics are off by default and run only if you opt in. On-chain activity (mints, Draws, Buybacks) is public by design — that is the blockchain, not data we collect. We never sell or share your data.

1. OVERVIEW & OUR APPROACH

Ticket4Life is a non-custodial interface (the “Interface”) to a set of public smart contracts (the “Protocol”) on Base. This Privacy Policy explains what data is, and is not, involved when you use the Interface. It expands on the summary shown on our site’s Privacy page.

Our approach is privacy by design. We built the Interface to function with the minimum possible information about you, and in most cases with none that identifies you at all. We do not maintain user accounts, we do not run identity checks, and we do not assemble profiles of the people who use the Interface. Where a feature needs to touch the outside world (loading fonts, reading a price feed, talking to the blockchain), we tell you plainly in this Policy what that involves.

Because the Protocol is a public blockchain application, some information is inherently public — but that is a property of the chain itself, not data we gather about you. We keep these two ideas separate throughout this Policy: what is public on-chain, and the very little we handle off-chain.

2. YOUR WALLET IS YOUR IDENTITY

When you connect a wallet to the Interface, your wallet address is the only identifier we work with. It is pseudonymous: it is a string of characters, not a person’s name, and it is not linked by us to any real-world identity.

- We never ask for your name, email address, phone number, postal address, or date of birth.
- We do not issue usernames, passwords, or logins. Connecting and disconnecting your wallet is the whole of “signing in.”
- We do not attempt to correlate your wallet address with your identity, your other wallets, or activity elsewhere.

Your wallet, and the private keys that control it, remain entirely yours. The Interface is a frontend only; it cannot access, move, freeze, or seize your assets or your Ticket, and it cannot recover lost keys.

3. WHAT WE DO NOT COLLECT

To be explicit, the Interface does not collect:

- **Personal identifiers** — no name, email, phone number, government ID, or KYC information of any kind.
- **Identity-linked analytics** — we do not tie analytics to who you are; the analytics described in Section 6 are pseudonymous, aggregated, and off by default.

- **Financial data beyond what is already public on-chain** — we do not take card numbers, bank details, or off-chain balances. Any transaction data associated with your use of the Protocol is the public on-chain record described in Section 4, not information we separately gather.
- **Stored location data** — the geo-check in Section 5 runs in memory and is never written down, stored, or transmitted by us as a record about you.

We do not build advertising profiles, and there are no advertising or marketing cookies anywhere in the Interface.

4. ON-CHAIN DATA IS PUBLIC

The Protocol runs on Base, a public Ethereum Layer-2 network. By design, interactions with the Protocol are recorded on a public ledger that anyone can read through a block explorer such as BaseScan. This includes, for example:

- minting a Ticket;
- Draws and prize payments;
- selling a Ticket back to the Protocol (the Buyback) or through the in-app marketplace.

This on-chain data is public because that is how a blockchain works, and it is not data we collect, control, or can delete. A public transaction is permanent and is visible to everyone. Your wallet address appears in these records; if you ever link that address to your identity elsewhere, third parties may be able to associate the two. That association happens outside the Interface and is not something we can prevent or reverse.

5. THE GEO-CHECK

The Interface runs a country-level eligibility check when the app loads. Its only purpose is to confirm that the Interface is not being made available in a restricted jurisdiction (see the Eligibility terms — for example Cuba, Iran, North Korea, Syria, Russia, Belarus, or any jurisdiction where prize-linked or crypto products are prohibited).

- The check is **country-level only** — it does not determine your precise location.
- It is performed **in memory** while the app loads.
- The result is **never stored, logged, or transmitted** by us as a record about you.

You remain solely responsible for complying with your own local laws, including confirming that you are of legal age and legally permitted to use prize-linked and crypto services in your jurisdiction.

6. ANALYTICS & CONSENT

The Interface uses Google Analytics 4 (GA4) operated under Google Consent Mode v2. This gives us a small amount of pseudonymous, aggregated usage data about how the Interface is used, so we can maintain and improve it.

- Analytics are **denied by default**. Nothing analytics-related runs unless you take action.
- Analytics run **only if you opt in** by accepting the “Analytics” cookie category in our consent banner.
- If you opt in, GA4 sets the cookies `_ga` and `_ga_*`. If you do not, these cookies are not set.
- Strictly-necessary local storage — your consent choice and your app preferences — is used to make the Interface work and to remember your decision. It is never transmitted.

This analytics data is aggregated and, although it is pseudonymous rather than truly anonymous (GA4 uses a client-ID cookie and may process technical data such as your IP address), we do not link it to your identity; we do not know who you are (see Section 2). You can change or withdraw your choice at any time through the consent controls. For the full breakdown of cookies and categories, see our Cookie Policy.

Legal basis, retention, and transfers. Where a data-protection law such as the GDPR applies:

- **Legal basis.** Our legal basis for analytics is your **consent**, which you give by accepting the “Analytics” category and can withdraw at any time. Our legal basis for strictly-necessary local storage (your consent choice and app preferences) is our **legitimate interest** in making the Interface work and remembering your decision, together with the strict necessity of that storage for a service you have requested.
- **Transfers.** GA4 and Google Fonts (Section 7) are provided by Google. When you opt in to analytics, or when the Interface loads fonts, the relevant technical data is processed by Google and may be transferred to and stored on servers in the **United States**, subject to Google’s own safeguards and privacy policy.

- **Retention.** If you opt in, GA4 retains this usage data for a limited, configured period — no longer than GA4’s maximum event-data retention of 14 months — after which Google deletes or aggregates it. Strictly-necessary local storage stays on your device until you clear it through your browser or withdraw consent. Off-chain, we hold no personal record of you to retain (see Section 2); on-chain data (Section 4) is public and permanent by the nature of the blockchain and is outside any retention control.

7. THIRD PARTIES

Like most web3 applications, the Interface relies on a small number of third-party services to function. When you use the Interface, these parties may receive limited technical information:

- **Google Fonts** — the Interface loads fonts from Google Fonts to render text, which involves a request to Google’s servers (see “Legal basis, retention, and transfers” in Section 6 regarding data processed by Google, including in the United States).
- **CoinGecko** — the Interface reads public price data from CoinGecko to display prices.
- **RPC providers** — to read the blockchain, the Interface connects to RPC providers, which may see your IP address, as with any web3 app.
- **Wallet providers** — the wallet you connect is operated by a third party with its own privacy policy governing how it handles your data.

We do not control these third parties, and their handling of any information they receive is governed by their own policies. We encourage you to review the privacy policies of your wallet provider and of any service you use alongside the Interface.

8. NO KYC / NO SELLING OF DATA

We want to be direct about two things:

- **No KYC.** We do not run “know your customer” or identity-verification processes. Your wallet address remains pseudonymous, and we do not ask you to prove who you are.
- **No selling or sharing.** We do not sell your data, and we do not share it for others’ advertising or marketing. There is no data brokerage of any kind, because there is essentially no personal data to broker.

The limited third-party interactions described in Section 7 are technical necessities of running a web3 interface, not a monetization of your information.

9. YOUR RIGHTS

Depending on where you live, data-protection laws (such as the GDPR or similar frameworks) may give you rights over personal data, including rights to access, correct, delete, or port it, to object to or restrict its processing, to withdraw a consent you have given, and to lodge a complaint with your local data-protection supervisory authority.

We respect these rights to the extent any applicable data-protection law applies. In practice, however, we hold no information that identifies you: no name, email, phone number, or account, and no stored location data. Because we do not know who you are and cannot connect a wallet address to a real-world identity, we are usually unable to locate a personal record to act on — there is none to retrieve or erase.

Three points follow from this:

- Off-chain, there is little or no identifying data for us to give you, correct, or delete, because we do not collect it. The main off-chain data governed by these rights is the pseudonymous analytics you may have opted into (Section 6), which you can switch off or withdraw at any time through the consent controls.
- On-chain data (Section 4) is public and permanent by the nature of the blockchain, and cannot be altered or removed by us or by anyone.
- Your right to lodge a complaint with a supervisory authority is unaffected: if you are in the EU or another jurisdiction with a data-protection regulator, you may contact that authority directly.

If you believe you have a data-protection request that applies to us, you may contact us using the details in Section 12, and we will respond consistently with applicable law.

10. CHILDREN

The Interface is not directed to, and is not for use by, minors. You must be of legal age in your jurisdiction and legally permitted to use prize-linked and crypto services in order to use the Interface.

We do not knowingly collect information from anyone under the applicable legal age. Because we collect no identifying information at all, we cannot verify age directly; the responsibility to confirm that you meet this requirement rests with you.

11. CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time to reflect changes to the Interface, the third parties it relies on, or applicable law. When we do, we will revise the "Last updated" date at the top of this document. Material changes will be reflected on the site's Privacy page. Your continued use of the Interface after an update means you accept the revised Policy.

12. CONTACT

Ticket4Life is a non-custodial interface to a public protocol. No legal entity, company, or jurisdictional base is claimed, and there is no fiduciary relationship.

If you have questions about this Privacy Policy, or wish to raise a data-protection request, you can reach us through the channels linked in the site footer:

- **X:** @Ticket4Life
- **Telegram:** link in the site footer

If a data-protection law applies to you, you also have the right to lodge a complaint directly with your local data-protection supervisory authority, in addition to contacting us.