

Privacy policy

Version 2.0 · Effective 6 October 2026 · Metarock Pty Ltd trading as DeStore Network · Byron Bay, NSW, Australia

In short: we collect what we need to run your account and your codes. When people scan a code, we count the scan by time, town and type of phone, and keep nothing that identifies them. Network addresses are only ever kept as keyed one-way codes. We do not sell or share personal information for advertising. You can ask to see, correct, export or delete what we hold about you.

1. Who we are

DeStore is run by Metarock Pty Ltd, trading as DeStore Network, of Byron Bay, New South Wales, Australia ("DeStore", "we", "us"). This policy covers the app at app.destore.network; the pages, QR codes, wallet passes and checkouts it hosts on destore.network and its subdomains; the website destore.network; and DeStore's apps inside other products: **DeStore – Free QR** and **DeStore Link QR** in Canva, and DeStore Events in ChatGPT. We follow the Australian Privacy Principles in the Privacy Act 1988 (Cth) and, where they apply to you, the EU and UK General Data Protection Regulations and US state privacy laws, including California's.

For your DeStore account and our own website we are the **controller** (the party responsible). For the people who scan a brand's codes or buy from a brand's page, we act for that brand as its **processor**, and the brand is responsible to them; we only use that information to provide the service to the brand.

2. What we collect, and where it comes from

From you, when you sign in and use DeStore

- **Account:** the email address or Google or Apple account you sign in with, the account number (a wallet address) created for you at sign-in, your profile picture if you add one, and which app you first arrived from.
- **Sign-in history:** when you sign in, and a short description of the device (for example "iPhone · Safari"). The network address is kept only as a keyed one-way code.
- **Your business:** its name, web address, logos, colours, fonts and voice, its products, and the people on your team and their roles.
- **What you make:** pages, codes, collections, uploaded files and pictures, QR styles, ticket and product settings, and what you type, say or upload to Clippy, DeStore's assistant.

- **Billing:** your credit balance and its history, your plan, and automatic top-up settings. Card payments are handled by Stripe; we do not see or keep your card number.
- **Support and contact:** what you send us by email or our contact forms.

From Canva

DeStore's Canva apps receive a Canva user and design identifier, used for fair-use limits and to remember which page a design made. They read only what each feature needs, when you use it: DeStore Link QR reads the words on the current page of your design; Free QR's "Save my brand" reads your brand kit's colours and the picture you select as your logo. Signing in from Canva uses Canva's sign-in; we never see your Canva password.

From ChatGPT

When you ask DeStore Events in ChatGPT to make a page, ChatGPT sends us the page's content. We do not receive your ChatGPT account details or the rest of your conversation.

From people who scan a code

For each scan we record the time, the town or city, state, postcode and country (worked out by our hosting network from the connection, never by asking for the phone's location), the type of phone, its operating system, browser and language, and the site that linked to it. To count people rather than scans, we make a daily visitor number from the connection and browser, using a secret key; it changes every day and cannot be turned back into either. We do not keep the network address or the full browser details. Link previews from social apps and search engines are not counted as scans.

From buyers of tickets and products

Payments are taken by Stripe or Square on the seller's own account. The buyer's name, email, card and address stay with the seller's Stripe or Square account. DeStore keeps the order's amount, what was bought and DeStore's fee and, for tickets, the ticket's number and whether and when it was checked in. If a buyer saves a ticket to Apple Wallet or Google Wallet, we keep what is needed to update it on their phone (a device identifier and push token from Apple, or Google's pass record).

From payment providers and partners

Stripe and Square tell us whether a payment succeeded and whether a seller's account can take payments. thirdweb confirms your sign-in.

3. Why we use it, and our legal basis

Purpose	Legal basis (GDPR / UK GDPR)
Running your account, hosting your codes and pages, counting scans for you, taking payments for your sales, and support	Performing our contract with you
Billing, tax and accounting records	Legal obligation

Keeping DeStore safe: preventing abuse, fraud, phishing and overuse (rate limits)	Legitimate interests (a safe service)
Improving DeStore, using counts rather than individuals	Legitimate interests (a better service)
Scan analytics for brands (as their processor)	The brand's legitimate interests in knowing how its codes are used
Anything we ask your permission for	Consent, which you can withdraw at any time

Where we rely on legitimate interests, you can object (section 9).

4. AI

Clippy and DeStore's apps send what you give them (your messages, photos, documents, the words of a Canva design, or a description of a screen) to **xAI** (Grok) and **Anthropic** (Claude) to write pages, read photos and documents, make pictures and speak replies. We use their business (API) services, which do not use what we send to train their models. AI does not make decisions about you that have legal or similarly significant effects. Automatic limits (such as rate limits and credit checks) only pause work; you can always contact us about them.

5. Who we share it with

We do not sell personal information and do not share it for cross-context behavioural advertising. We share it only with providers that help us run the service, each of which receives only what it needs for its part:

Provider	What for
Cloudflare	Hosting, databases, file storage, scan counting, page screenshots
Vercel	Hosting the app and its server functions
thirdweb	Sign-in and account numbers
Stripe, Square	Payments, top-ups, plans, sellers' payouts
xAI, Anthropic	AI (section 4)
Apple, Google	Wallet passes; Google also for address search and sign-in with Google
Canva, OpenAI	When you use our apps inside Canva or ChatGPT
Resend, SendGrid, n8n	Sending emails such as invites, receipts and invoices
Web3Forms	Our website's contact form

jsDelivr, esm.sh, Google Fonts, Esri	Code libraries, fonts and maps loaded by your browser inside the app (they see your browser's connection, not your account)
--------------------------------------	---

We may also disclose information if the law requires it, to protect people from harm or fraud, or to a business that takes over DeStore, which must keep to this policy.

Brands may add their own analytics to pages they publish. They are responsible for telling their visitors about it.

6. Overseas

Our providers store or process information in Australia, the United States, the European Union and other countries. Where information leaves Australia, the EU or the UK, we rely on our providers' contractual commitments, including the European Commission's standard contractual clauses and the UK addendum where they apply, and we take reasonable steps so that they handle it consistently with the Australian Privacy Principles.

7. Public blockchain records

Some product codes are recorded on a public blockchain (Soneium) so their history can be checked. These records hold product and code details and the brand's account address, never a person's name or contact details. Anything on a public blockchain is public and cannot be changed or deleted.

8. How long we keep it

Information	Kept for
Account, business details and what you make	While your account is open; deleted within 90 days of closing it, except what the next rows need
Billing, credit ledger and sales records	5 years, as Australian tax law requires
Sign-in history	12 months
Detailed scan records	90 days; counts that identify no one may be kept longer
Unpublished previews	7 days
Rate-limit counters	Minutes to one day
Wallet pass registrations	Until the pass is removed from the phone or its event is over
Sign-up enquiries (sales leads)	2 years
Public blockchain records	Permanent (section 7)

9. Your rights

Wherever you live, you can ask us to:

- tell you what personal information we hold about you and give you a copy (including in a portable format);
- correct it;
- delete it, or close your account;
- stop using it for a purpose based on legitimate interests or consent, or restrict how we use it.

Email josiah@destore.network. We will reply within 30 days (within one month where the GDPR applies) and will not charge you or treat you differently for asking. We may need to confirm who you are first. If we cannot do what you ask, for example because the law requires us to keep a record, we will say why.

California residents have the right to know, delete and correct personal information, to opt out of its sale or sharing (we do neither), to limit the use of sensitive personal information (we collect none for that purpose), and not to be discriminated against for using these rights. You can use an authorised agent.

If you scanned a brand's code or bought from a brand's page, the brand is responsible for that information. We will pass your request to them and help them answer it.

10. Cookies and browser storage

- The app keeps your sign-in and settings (such as theme and recent choices) in your browser's storage. These are needed for the app to work.
- The sign-up page remembers, for that browser tab only, which version of its heading it showed you, while we test which works best.
- DeStore Link QR in Canva remembers, in Canva's app storage, which page each design made.
- DeStore sets no cookies, and uses no advertising or cross-site tracking. The sign-in service (thirdweb) keeps your session in your browser's storage.

11. Security

We protect information with encryption in transit (HTTPS everywhere), access limited to each account's own data, keyed one-way codes in place of network addresses, sealed (encrypted) storage of payment-provider tokens, sandboxed frames for page code, and limits against abuse. No system is perfectly secure. If a data breach is likely to cause serious harm, we will tell the people affected and the Office of the Australian Information Commissioner as the Notifiable Data Breaches scheme requires and, where the GDPR applies, the relevant supervisory authority within 72 hours of becoming aware of it. To report a security problem, email josiah@destore.network.

12. Children

DeStore accounts are for people 18 and over. The service is not directed at children under 16, and we do not knowingly collect their personal information. If you think a child has given us personal information, email us and we will delete it.

13. Complaints

Email josiah@destore.network first. We will reply within 30 days. If you are not satisfied, you can complain to:

- Australia: the Office of the Australian Information Commissioner, oaic.gov.au;
- the European Union: the data protection authority where you live or work;
- the United Kingdom: the Information Commissioner's Office, ico.org.uk;
- elsewhere: your local privacy regulator.

14. Changes

We may update this policy as the service or the law changes. We will tell you about a material change by email or in the app before it takes effect. The date at the top shows the current version.

Questions about this document: josiah@destore.network · destore.network