Brydg
Privacy Policy

Version [1.0] · Effective [DATE] · Controller: [OPERATING ENTITY], [address] ("Brydg", "we") · Contact: [privacy email] · [DPO / representative if required: name, contact]

> **DRAFT FOR LEGAL REVIEW, NOT FOR PUBLICATION**
>
> Working draft for counsel. Drafted GDPR-first (the strictest widely applicable baseline) with placeholders; counsel must confirm controller identity, jurisdictional add-ons (PDPA-type regimes in target corridors), retention periods against applicable AML law, and the international-transfer mechanism. The pre-sale is not offered in Singapore, the United Kingdom or the GCC states, so UK GDPR, the Singapore PDPA and GCC data-protection regimes apply only to the extent residual data from blocked access attempts is processed.

1. What this covers

This policy explains how we process personal data when you use the Brydg pre-sale site, create an account, complete verification, purchase Token allocations, use the referral programme, contact support, or subscribe to updates. The Terms of Sale govern purchases; this policy governs data.

2. What we collect

- **Account data:** email, password hash, country, language, communication preferences.
- **Eligibility and attestation data:** the country of residence you declare, your attestation at each quote and purchase that you are not resident in, located in, or purchasing on behalf of anyone in a Restricted Jurisdiction (Singapore, the United Kingdom, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates, and any jurisdiction added later), and the time and Terms version of each attestation. Where required, evidence of residence.
- **Verification data (tiered by purchase amount):** name, date of birth, nationality, address, government identity document images, selfie, and at higher tiers source-of-funds or source-of-wealth documentation; outcomes of reviews.
- **Wallet and transaction data:** wallet addresses you link, signed ownership messages, transaction hashes, amounts, chains, deposit addresses, screening results. Blockchain transactions are public by design and permanently visible on-chain; we cannot erase on-chain data.
- **Purchase and ledger data:** allocations, stages, prices, terms versions, referral relationships, claims.
- **Support and communications:** messages, the "I already sent funds" form, complaint records.
- **Technical data:** IP address, approximate location derived from it (used to enforce the Restricted Jurisdictions at access and at quote, and to detect location-masking tools), device and browser data, and cookie data per §9.
- We do **not** collect: private keys, seed phrases or wallet PINs. Never provide them to anyone claiming to be us.

3. Why we process it (purposes and legal bases, GDPR Art. 6)

PURPOSE	LEGAL BASIS
Providing the account, dashboard, purchases, delivery at TGE, distributions	Contract (Art. 6(1)(b))

PURPOSE	LEGAL BASIS
Identity verification, sanctions and wallet screening, AML/CTF compliance, enforcement of the Restricted Jurisdictions and the eligibility attestation	Legal obligation (6(1)(c)); where a check exceeds strict obligation, legitimate interests (6(1)(f)) in lawful operation
Fraud prevention, referral-abuse detection, detection of location masking, security, access logging	Legitimate interests (6(1)(f))
Support, notices, terms-version notifications	Contract / legitimate interests
Newsletter and marketing updates	Consent (6(1)(a)), withdrawable any time via unsubscribe
Regulatory reporting, tax reporting, responding to lawful requests	Legal obligation
Establishing or defending legal claims, including in relation to a false eligibility attestation	Legitimate interests

We use identity documents for verification and compliance, **not marketing**. We do not sell personal data. We do not use your data for automated decisions producing legal effects without human review: verification decisions at document tiers are made by humans; automated screening and jurisdiction flags route to human review.

4. Who receives it

Service providers under contract (hosting, cloud storage, email delivery, blockchain analytics and screening, IP geolocation, and, if engaged, an identity-verification provider); our external legal counsel and accountants; auditors; payment and settlement infrastructure; regulators, tax authorities, law enforcement and courts where required; and a successor entity in any reorganisation (with notice). Providers act on our instructions; a current provider list is available on request.
[Populate at launch: hosting, R2 storage, Brevo, analytics and screening vendor, geolocation vendor, Sumsub if engaged.]

5. International transfers

We operate from [jurisdiction] and use providers in multiple countries. Where data leaves a jurisdiction with transfer restrictions (for example the EEA), we rely on
[adequacy decisions / standard contractual clauses / equivalent safeguards]; copies are available on request.
[Counsel: confirm mechanism per provider.]

6. Security

Identity documents are stored encrypted; access is only via short-lived signed links; every access is logged. Role-based access, separated admin realm with 2FA, least-privilege support roles, and monitored infrastructure. No system is perfectly secure; we will notify you and the relevant authority of a breach where the law requires.

7. Retention

- Account, ledger and attestation data: for the life of your participation **plus [5 to 10] years** (AML and audit obligations; ledger data also underpins your allocation and delivery rights; attestation records evidence eligibility at each purchase).
- Verification documents: **[5] years** after the relationship ends, or longer where law requires.
  [Counsel: fix per applicable AML law.]
- Marketing data: until you unsubscribe.

- Technical logs, including geolocation results: [12 to 24] months.
- On-chain data: permanent by nature; outside our control.

8. Your rights

Subject to law, you may request: access to your data; correction; erasure; restriction; portability; and objection to legitimate-interests processing. You may withdraw consent (marketing) at any time. **Limits:** we cannot erase data we must keep for AML, tax, eligibility-evidence or ledger-integrity purposes, and we cannot alter blockchains. Requests: [privacy email]; we respond within [one month]. You may complain to your supervisory authority [EEA: your local DPA; identify lead authority if any].

9. Cookies

Strictly necessary cookies (session, security, jurisdiction enforcement) run without consent. Optional analytics run only with consent via the banner; we use [tool, keep minimal; prefer cookieless analytics]. We do not run advertising cookies. Full cookie table: [list at launch].

10. Children

The services are for adults 18+. We do not knowingly process children's data; accounts found to belong to minors are closed and data deleted subject to legal holds.

11. Changes

We may update this policy; changes are published on Official Channels before taking effect, with material changes notified to account holders. The version and effective date appear at the top.