PRIVACY POLICY

LAST UPDATED: DECEMBER 05, 2025

1. INTRODUCTION

Until the incorporation and operational onboarding of the Emyo issuing entity (Emyo Ltd. or such other group company as identified in the Whitepaper and these Privacy Policy), the Site and any preliminary whitelisting / waitlisting forms, expressions of interest, and related investor or user queries will be administered on its behalf by ToyKarma Inc., a Wyoming corporation with registered office at 30 N Gould St, Sheridan, WY 82801, United States. During this interim period ToyKarma Inc. acts solely as an administrative and technology service provider and first-line contact point for such queries and whitelisting processes and does not itself issue Tokens, enter into SAFTs, or provide regulated financial, investment, or gaming services; once the Emyo issuing entity confirms that it has assumed direct control of the Emyo Services, all such responsibilities automatically transfer to it, and all prior whitelisting communications and expressions of interest handled by ToyKarma Inc. shall be deemed to have been made on behalf of that Emyo entity.

This Privacy Policy describes how **ToyKarma Inc.** ("**we**", "**us**", "**our**", "**Emyo**" or the "**Company**"), collects, uses, stores, and protects information when users access the Emyo website (the "**Website**"), dashboard, token-related interfaces, loyalty system, or any other services we operate (collectively, the "**Services**", "**Company Services**" or "**Emyo Services**").

We are committed to protecting the privacy of our users and to handling data in a lawful, transparent, and secure manner. We operate under the legal framework applicable in the BVI, including the **Data Protection Act, 2021**, the **Anti-Money Laundering Regulations**, and relevant compliance obligations, our Services are **not intended** for users located in jurisdictions requiring EU General Data Protection Regulation (GDPR), U.S. California Consumer Privacy Act (CCPA), or equivalent enhanced data-protection regimes. Access for such users may be restricted or disabled through geo-blocking, eligibility screening, or limitations of functionality.

This Privacy Policy applies solely to the Emyo Services and the digital infrastructure supporting the **Emyo Coin**. It does not apply to any third-party platforms, partner-operated gaming environments, or external websites that may be accessible through our interfaces. Users are encouraged to review the privacy policies of such third-party platforms independently.

By accessing or using the Services, connecting a wallet, participating in the Loyalty Program, or interacting with the Emyo Coin, you acknowledge and agree to the collection and processing of information as described in this Privacy Policy.

We may revise this Privacy Policy from time to time to reflect updates to our Services, technological changes, or regulatory requirements. The "Last Updated" date at the top of this page indicates the most recent version.
Continued use of the Services following any update constitutes acceptance of the revised Policy.

If you do not agree with this Policy, you should discontinue access to the Services immediately.

Our full company details are:

Legal entity name: ToyCarma Inc.
The name and physical address of the legal entity: Northwest Registered Agent Service Inc, 30 N Gould St Ste N, Sheridan, WY 82801
Email address: legal@emyo.io

2. DEFINITIONS

Defined Terms. For the purposes of this Privacy Policy (the "**Policy**"), the following terms shall have the meanings set out below. These definitions are tailored to the operational and legal structure of the Company Services. The Emyo Services are not intended for users located in jurisdictions where GDPR, CCPA, or comparable enhanced data-protection regimes apply; therefore, references to such legislation are provided for descriptive clarity only and shall not be deemed applicable to the Company:

"**Account**" means a User profile created within the Emyo platform or linked through wallet authentication, including associated identifiers, settings, and activity data.

"**Aggregated Data**" or "**Anonymized Data**" means information that has been processed such that it no longer identifies any individual.

"**Blockchain Data**" means publicly available on-chain information such as wallet addresses, transaction hashes, timestamps, staking activity, and smart-contract interactions.

"**Cookies**" or "**Tracking Technologies**" means cookies, pixels, tags, local storage objects, or similar technology used to operate, secure, personalize, or analyze the Services.

"**Data Controller**" means the Company, insofar as it determines the purposes and means of Processing Personal Data providing Services in accordance with the BVI Data Protection Act, 2021.

"**Data Processor**" means any third party engaged by the Company that Processes Personal Data on behalf of the Company and in accordance with its documented instructions.

"**KYC/AML Information**" means information collected from Users where required under applicable anti-money laundering, counter-terrorist financing, or sanctions-compliance obligations.

"**Loyalty Program**" means the promotional and utility-based rewards system operated by the Company in accordance with the applicable Loyalty Program Terms.

"**Personal Data**" (or "**Personal Information**") means any information relating to an identified or identifiable natural person, including data that can directly or indirectly identify you (such as your name, contact details, identification number, or online identifiers).

"**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, or erasure.

"**Supervisory Authority**" (or "**Regulatory Authority**", where applicable) means an independent public authority or government agency responsible for monitoring and enforcing compliance with data protection and privacy laws.

"**Third-Party Service**" means any external product, tool, application, software, infrastructure provider, or service operated by an independent third party that supports, integrates with, or interacts with the Company. This includes, without limitation, KYC/AML verification providers, hosting and cloud infrastructure, analytics and security tools, wallet-connection providers, blockchain infrastructure services (such as RPC nodes, blockchain explorers, or indexing services), and communication or marketing delivery platforms. Third-Party Services may process only the Personal Data strictly required to perform their functions on behalf of the Company and may not use such data for their own purposes.

"**Token Generation Event**", "**TGE**", or "**Token Sale**" means the generation and any public or private offering, sale, distribution of the Tokens by the Company on such a blockchain protocol or network as the Company may determine from time to time in its sole discretion.

"**Token(s)**" or "**Emyo Token**" or "**EMYO**" means the cryptographic utility tokens generated by the Company at the Token Generation Event for the purpose of enabling access, payments, loyalty interactions, fee mechanics, user reward functions, and other strictly functional utilities within the Emyo transactional and loyalty framework, including (where permitted) casino-related payments,

loyalty tier accumulation, staking, in-protocol reward redemption, on-platform spend, and internal settlement or conversion logic. For the avoidance of doubt, the Tokens do not represent or confer any equity, ownership, security, revenue share, economic interest, expectation of profit, cashflow rights, or any participation in the business, assets, goodwill, or results of operations of the Company or any affiliate, and are not intended for investment.

"**User**" means any natural person who accesses or uses the Website or Services, whether or not such person registers an Account ("you", "your").

"**Wallet Address**" a public blockchain address used to interact with Emyo smart contracts or interact with the Emyo Coin.

"Waitlist" or "Whitelist" means the pre-registration process operated by the Company for Users who express interest in participating in the Token Sale or related token-allocation events. The Waitlist may require Users to submit certain Personal Data (such as name, email, communication handle, country of residence, and Wallet Address) in order to (i) verify eligibility and geographic restrictions, (ii) conduct compliance and risk checks, (iii) administer prioritization or allocation tiers, and (iv) communicate with Users regarding Token Sale participation, instructions, or updates. Participation in the Waitlist does not guarantee eligibility, allocation, or the right to participate in the Token Sale.

3. INFORMATION WE COLLECT

3.1 We may collect and process various categories of Personal Data necessary for the operation, security, and improvement of the Emyo Services. These categories include, but are not limited to, the information described in the following sections.

3.2 **Information You Provide.** You may provide certain information when accessing or using the Services, including the Loyalty Program, staking modules, dashboards, support channels, or promotional features. This may include:

(a) **Contact information:** Email address, username or display name, phone number, communication preferences, and other information enabling us to contact you personally.

(b) **Account information:** Account ID, Wallet Address(es), Account creation/modification timestamps, platform settings and preferences, authentication credentials (such as passwords or other security information).

(c) **Optional Identification / Verification Data**. Where required for eligibility-restricted functions, AML/CTF compliance checks, offline-online linkage, higher-risk activities, or other regulatory purposes, we may collect: full name, date of birth, address, residency or citizenship information, phone number, gender, title, occupation status and title, government-issued identification (e.g., passport, ID card, driver's license), proof of address, copies of tax or other government documents, tax identification or reference numbers, national identification numbers (e.g., social security, taxpayer, resident or similar numbers), KYC details, demographic information, credit or suitability information (including credit reports and suitability responses), and other information related to your identity or eligibility.

(d) **Financial Information:** Bank account details, payment instrument information, transaction references, and related information used to process payments, refunds, or payouts.

(e) **Token Sale and Loyalty Program Participation Data:** Information relating to your participation in any Token Sale, staking, or Loyalty Program, such as whitelisting or eligibility status, allocation tier, contribution currency and amount, vesting and unlock schedules, reward points or tiers, and Wallet Addresses designated for token or reward receipt. Where such data overlaps with Account Information, Financial Information, or Blockchain Data, it is processed in line with those categories.

(f) **Media and Biometric Information:** Selfie photos, images, videos (including audio recordings), and biometric identifiers or templates derived from such media (including facial

geometry or similar biometric information) that are used for identity verification, fraud prevention, or security purposes.

(g) **Communication Data**: Support tickets and emails, feedback messages, requests and inquiries, survey responses and other communications with us.

(h) **Social Media, Online Presence, and Social Data:** References or links to your social media accounts, personal websites, blogs, or other online presence materials that may identify you; public-facing profile information on the Services; messages and other communications you may send to other users through the Services; identity and contact information of friends or contacts you choose to refer to our Services; and any other user-generated content or material you post on the Services that contains Personal Data and does not fall within the other categories described here. **Please be aware that when you use certain social or interactive features in the Services (such as messaging other users or commenting publicly), any personal information you provide may be visible to other users and may be considered "public" (unless otherwise required by applicable law). You should exercise caution before sharing information that you wish to keep private**.

(i) **Marketing and Communications Preferences:** Data related to your marketing and communications preferences, including your choices regarding newsletters, product updates, promotional offers, and other marketing communications from us or our partners, as well as records of your opt-in/opt-out decisions. We retain certain information as needed to respect and implement your preferences.

(j) **Professional, Financial, Investment, and Transactional Data (where required).** In limited cases, and only where required by applicable law, our AML/CTF obligations, risk management policies, or by our banking/payment partners, we may ask you to provide additional information. This may include:

(i) Cryptocurrency addresses, Wallet Address and blockchain transactional data associated with your use of the Services;

(ii) Traditional payment details and historical transaction data related to deposits, purchases, and payouts processed through the Services; Basic employment and professional information (such as employer, role, industry) and, where necessary, documents evidencing source of funds or source of wealth (e.g., payslips or income confirmations, company documents, or similar records);

(iii) Information regarding your traditional investment or cryptocurrency experience, objectives, risk tolerance, and preferences, where needed to assess eligibility or risk;

(iv) Net asset or liability information and tax-related information required for reporting to competent tax authorities, to the extent required by law.

(v) We request such information **only where strictly necessary** to comply with legal and regulatory requirements, to complete enhanced due diligence, or to protect the integrity and security of the Services. It is not collected from all users by default.

(k) **Voluntary Information.** Any other information you choose to provide when interacting with the Services.

By providing us with selfie images or videos, identification documents, or other media for verification, you acknowledge and consent to our extraction, analysis, storage, and processing of the biometric information contained therein (including facial geometry data) and of the underlying images and video, as described in this Privacy Policy.

3.3 **Information We Collect Automatically.** When you access or use the Services, we may collect information automatically to ensure security, functionality, performance, and user experience.

(a) **Technical Data / Online Identifiers:** IP address, device type and model, browser type and version, browser plug-in types and versions; operating system and platform; language and locale; timezone setting and approximate location; session identifiers; access logs and timestamps; other diagnostic and technical data.

(b) **Mobile Device Data:** If you access the Services via a mobile device, we may collect information such as: type of mobile device, mobile operating system and version, mobile browser type, mobile device unique ID, IP address of the mobile device, and other mobile device identifiers or technical information.

(c) **User / Usage Data**: Login attempts (successful and failed); authentication and security events; pageviews and navigation patterns; click-stream data; interaction logs (including buttons clicked, features used, and in-app events); time and date of visits; time spent on pages or in specific views; error reports and crash/diagnostic data; session duration and frequency of use.

(d) **Geolocation Data:** Subject to your device and browser settings, we may collect or derive approximate geolocation information (e.g., based on IP address or device settings) for security, fraud prevention, analytics, and localization.

(e) **Blockchain Data**: Because Emyo operates in a Web3 environment, interactions with our smart contracts may involve publicly available blockchain information, including: Wallet addresses, transaction hashes, staking and on-chain activity, block timestamps, contract interaction metadata. We do not store private keys, seed phrases, or other sensitive wallet credentials.

(f) **Cookies and Similar Technologies:** We may use cookies, pixels, tags, and local storage objects to: operate the site, enable authentication, enhance functionality, analyze performance and usage.

(g) **Behavioral Data**: Data we may derive or assume related to your behavior, usage, interests, and other activity.

3.4 **Information Obtained From Third Parties**. We may receive information from approved third-party sources where necessary for operating or securing the Services.

(a) **Verification & Compliance Partners.** Used only where verification is required: identity confirmation data, sanctions and AML screening data, address validation, watchlist match indicators, and related compliance information.

(b) **Analytics or Performance Partners:** Traffic attribution data, campaign performance metrics, general usage analytics, and similar aggregate or pseudonymous statistics.

(c) **Public Blockchain Sources:** On-chain activity analysis, transaction pattern analysis, and anti-fraud or risk-scoring data based on publicly available blockchain information.

(d) **Affiliate or Referral Partners:** Referral IDs, campaign source, and basic attribution metadata related to referral or affiliate programs.

3.5 **Information We Do Not Collect**. To avoid misunderstanding:

(a) We do not collect or store private keys or seed phrases, or online banking passwords;

(b) We do not intentionally collect "special categories" of personal data such as health information, religious or philosophical beliefs, trade union membership, or detailed political opinions, except where required by law and subject to appropriate safeguards;

(c) We do not knowingly collect personal data from children where such collection is prohibited by applicable law.

4. HOW WE USE YOUR INFORMATION

4.1 We collect and process your Personal Information lawfully, fairly, and without intrusiveness, solely for the operation of our platform and in order to comply with applicable legal requirements. We use your information for the following purposes:

- **(a)** To verify your identity (KYC) and perform AML/CTF checks, ensuring compliance with applicable regulations;
- **(b)** To process your registration and maintain your Account, including access to platform features, loyalty programs, and related functionality;
- **(c)** To provide, operate, and improve our services, including personalization of your experience, optimization of platform performance, and development of new features;
- **(d)** To authenticate you as a User, maintain security, detect fraud, prevent multi-accounting, and ensure the integrity of the system;
- **(e)** To conduct internal analytics, including demographic profiling, statistical analysis, and aggregated reporting to improve business operations;
- **(f)** To respond to your questions, comments, support inquiries, or other requests;
- **(g)** To comply with our contractual, legal, and regulatory obligations, including reporting duties and lawful disclosures;
- **(h)** To take appropriate action if unlawful activity or serious misconduct is suspected, including investigation, account review, suspension, or cooperation with authorities;
- **(i)** To administer any Token Generation Event, including whitelisting, allocation, vesting and unlock tracking, distribution of Tokens, and related recordkeeping;
- **(j)** To operate the Loyalty Program, including calculating and issuing rewards, tracking participation, enforcing program rules, and preventing abuse or multi-accounting in connection with reward activities;
- **(k)** To contact you regarding your eligibility, to administer the Waitlist, and to comply with geographic, regulatory, sanctions-related, or eligibility restrictions applicable to the Token Sale.
- **(l)** To establish, exercise, or defend legal claims, if necessary.

4.2 We may use your information for marketing and promotional purposes, including sending updates, offers, and news. You may opt out of marketing communications at any time during registration or via unsubscribe options in any message.

4.3 **Disclosure of Personal Data.** We do not sell or commercially distribute your personal data.

5. LEGAL GROUNDS FOR THE PROCESSING

5.1 We process your Personal Data only where we have a valid legal basis and act as a data controller when determining the purposes and means of such Processing. We rely on four grounds: consent, contract, legal obligation, and legitimate interests.

5.2 **Consent** applies where you freely agree to specific Processing activities, such as receiving marketing communications or enabling optional analytics or non-essential cookies. You may withdraw consent at any time without affecting the lawfulness of prior Processing.

5.3 **Contract** serves as a basis where Processing is necessary to provide the Emyo Services, administer any Token Sale, create and maintain your Account, enable platform features and the Loyalty Program,

or take steps at your request before entering into an agreement. Without such data, certain Services cannot be provided.

5.4 **Legal obligations** require us to Process data for compliance purposes, including KYC/AML checks, sanctions screening, recordkeeping related to Token Sale participation and, where required, Loyalty Program rewards, responding to lawful requests from authorities, and other obligations necessary for the operation of the platform and for compliance with applicable law.

5.5 **Legitimate interests** allow us to Process data necessary to operate, maintain, and improve the Services; ensure security and prevent fraud or multi-accounting; conduct internal analytics; provide support; and protect our rights, Users, and platform integrity. We rely on this basis only where these interests are not overridden by your rights and freedoms.

Table 1. Legal Grounds for the Processing

Type of Data	What do we do?	Why do we do it?	What is the Legal Basis?
Identity, Contact and Account Data (Contact information, Account information, Wallet Address, Marketing and Communications Preferences)	Register and maintain your Account; link your Wallet; manage access to dashboards, Loyalty Program and token-related interfaces; communicate with you about your Account and the Services.	To provide, operate, and administer the Emyo Services; to allow you to log in, use platform features, receive service notices and essential communications.	**Performance of a contract**: necessary to provide the Services you request. **Legitimate interests**: to ensure we can communicate with Users and operate the platform efficiently.
KYC/AML and Verification Data (Optional Identification / Verification Data, Professional / Financial / Investment data where required, Media and Biometric Information, information from Verification & Compliance Partners)	Verify your identity, perform KYC/AML and sanctions checks, assess eligibility and risk, confirm source of funds/wealth where required, prevent fraud and multi-accounting.	To comply with anti-money-laundering, counter-terrorist-financing, sanctions and other regulatory requirements; to protect the integrity of the platform and prevent abuse.	**Legal obligation**: compliance with AML/CTF, sanctions and similar rules. **Legitimate interests**: to safeguard the Services from fraud and abuse.
Financial, Transactional and Token-Sale / Loyalty Data (Financial Information, Token Sale and Loyalty Program Participation Data, relevant Blockchain Data)	Process deposits, purchases, payouts and refunds; administer any Token Generation Event (whitelisting, allocation, vesting/unlock and distribution); operate	To execute and record token purchases and related transactions; to maintain accurate records of Token Sale participation; to calculate and deliver Loyalty rewards and other on-platform	**Performance of a contract**: necessary to perform payment, Token Sale and Loyalty Program obligations. **Legal obligation**: record-keeping where required by law or for

	the Loyalty Program, calculate and credit rewards, track participation and enforce program rules.	utility functions.	tax/financial compliance. **Legitimate interests**: to ensure financial integrity and accurate internal accounting.
Technical, Device, Usage, Geolocation, Cookies and Behavioral Data (Technical Data / Online Identifiers, Mobile Device Data, User / Usage Data, Geolocation Data, Cookies and Similar Technologies, Behavioral Data, data from Analytics or Performance Partners)	Operate and secure the Website and dashboards; log access and sessions; troubleshoot incidents; monitor performance; run analytics and statistics; remember preferences; improve layout and features.	To keep the Services functioning, secure and reliable; to understand how Users interact with the platform; to improve usability, performance, and product decisions. Please check our Cookies Policy for further details.	**Legitimate interests**: to run, protect, and improve the Services and IT infrastructure. **Consent**: for non-essential Cookies, analytics or tracking where required.
Communication and Support Data (Communication Data, including emails, support tickets, in-product messages, feedback and survey responses)	Provide customer support; respond to questions and complaints; handle requests related to your Account, Token Sale participation or Loyalty Program; collect feedback and improve the user experience.	To resolve issues, maintain service quality and develop the platform based on User feedback.	**Performance of a contract**: necessary to support Users of the Services. **Legitimate interests**: to ensure effective customer care and service improvement.
Waitlist Data (Name or display name, email address, social media username (such as Telegram or X(Twitter)), country of residence, Wallet Address designated for potential participation in the Token Sale)	Process Waitlist submissions; verify eligibility and geographic restrictions; manage waitlist or whitelist status; contact Users with relevant Token Sale notifications and instructions; prevent ineligible participation, fraud, or multi-accounting.	To administer Waitlist participation; to ensure Users meet geographic and regulatory requirements; to prepare Token Sale allocation processes; to communicate essential information related to the Waitlist and Token Sale.	**Legitimate interests:** to operate and secure the Waitlist and ensure eligibility. **Legal obligation:** compliance with geographic, sanctions, fraud prevention and eligibility restrictions. **Consent:** for optional marketing communications.

5.6 **Right to withdraw Consent**. Where Processing is based on consent, you may withdraw it at any time by contacting us using the details in this Policy. Withdrawal does not impact the lawfulness of Processing carried out before that moment.

5.7 **Automated Decision-Making**. We do not engage in automated decision-making or profiling that produces legal or similarly significant effects. If such methods are introduced later, they will comply with applicable law and include safeguards such as the right to request human review and to contest automated decisions.

6. INFORMATION SHARING

6.1 Your information may be shared only with the categories of recipients described below and solely for the purposes set out in this Privacy Policy and the applicable Token Sale documentation. We may share your Personal Data with:

(a) **Business partners, suppliers, and service providers.** This includes third parties that perform specific operations necessary for the functioning of the Emyo Token Sale and related Services, for example: KYC/AML and sanctions-screening providers, identity verification and risk-scoring tools used to verify your eligibility and comply with legal requirements; hosting, cloud, security, and infrastructure providers that operate our websites, dashboards, and back-end systems; analytics and performance tools that help us understand how the Token Sale interfaces are used and improve them; wallet-connection, launchpad, whitelisting, allocation, vesting, and token-distribution providers where applicable; payment, exchange, and on-/off-ramp partners facilitating contributions or settlements connected to the Token Sale.

(b) Authorized employees and contractors. Authorized employees, consultants, and contractors of the Company (and, where relevant, of its Affiliates) who need access to Personal Data to perform their duties, operate the Token Sale, provide support, or carry out compliance and risk-management functions.

(c) Affiliates and group companies. Our parent entities, subsidiaries, and other entities under common control, where reasonably necessary for internal administration, compliance, audit, risk management, or to operate the Token Sale and related Services within the broader Emyo ecosystem.

(d) **Regulators or authorities, and other third parties for legal reasons.** Regulators, law-enforcement bodies, tax and supervisory authorities, courts, and similar public bodies where disclosure is required by applicable law, regulation, court order, or lawful request, or where we consider it reasonably necessary to protect our rights, enforce our Terms, or investigate fraud, abuse, or security incidents. These recipients act under their own legal powers and are not bound by our instructions.

(e) Parties to corporate transactions. Potential or actual buyers, investors, and their advisers in connection with any merger, acquisition, investment, restructuring, sale of assets, or similar corporate transaction involving the Company or the Emyo Token Sale, to the extent permitted by law. In such cases, we seek to ensure an appropriate level of protection for your Personal Data.

(f) Third parties you connect or interact with. Where you choose to connect your Wallet or Account to a third-party launchpad, exchange, portfolio tracker, marketing or community platform, or other application and instruct us or technically enable us to share information with such third party. Once you authorize such sharing, the third party's use of your information is governed by its own privacy policy, and the Company is not responsible for its practices. Revoking access or disconnecting your Wallet or Account will not affect information the third party has already received; any request to delete such information should be addressed directly to that third party.

(g) Aggregated and anonymized data. We may share Aggregated or Anonymized Data with partners, service providers, or the public (for example, high-level statistics about participation in the Token Sale or ecosystem usage). Such information does not identify any individual.

6.2 All third parties referred to in points (a), (b), (c), (e), (f), and (g), other than regulators and public authorities acting under their own legal powers, process Personal Data only on the Company's instructions and are bound by confidentiality and appropriate data-protection obligations. By using the platform and participating in the Token Sale, you consent to these processing and sharing activities as described in this Privacy Policy.

7. THIRD-PARTY SERVICES

7.1 We may use Third-Party Services that support the operation, security, and functionality of Services. These service providers may access certain Personal Data only to perform their tasks on our behalf and must process it strictly in accordance with our instructions and contractual obligations. They are not permitted to use your information for their own purposes.

7.2 The Emyo Services may include integrations with external solutions such as KYC/AML providers, hosting and infrastructure providers, analytics tools, wallet-connection services, or security and risk-monitoring tools. Certain features may rely on blockchain infrastructure providers, including RPC nodes or indexing services.

7.3 If you interact with third-party wallet providers (e.g., MetaMask, Trust Wallet or similar), any information you provide to those providers, including Wallet Addresses, device data, or connection details, is processed under their respective privacy policies. The Company does not control how such providers collect or use information outside of the Company's scope of Services.

7.4 Because blockchain transactions are public by design, certain information (such as Wallet Addresses, transaction hashes, and on-chain activity) may be visible through blockchain explorers or third-party indexing services. This visibility is inherent to blockchain technology and is not controlled by the Company.

7.5 We may work with marketing or communication partners for optional promotional activities. These partners receive only the information necessary for the specific function (for example, anonymized analytics or technical delivery of communications) and cannot use it for unrelated purposes.

7.6 We may also share Aggregated or Anonymized Data with partners or service providers. Such information does not identify any individual.

7.7 If you choose to use third-party applications, websites, or platforms connected to or accessible from Emyo Services, the data you provide to them is governed by their own privacy policies. The Company is not responsible for the practices of such Third-Party Services. Revoking access or disconnecting an integration within the Emyo Services does not affect information that the third party has already obtained; any request for that third party to delete or update your information must be addressed to that third party directly.

8. DATA SECURITY

8.1 We implement technical and organizational measures to protect personal data, including encryption, access controls, monitoring systems, smart-contract transparency, and compliance procedures aligned with BVI regulatory expectations. These measures reflect the requirements described in the BVI Data Protection Act, 2021, and correspond to the operational model outlined in the legal analysis of the Company.

8.2 Although we apply commercially reasonable security standards, no system of electronic transmission, storage, or blockchain-based interaction can be guaranteed as fully secure. Users remain responsible for the security of their own devices, networks, and self-custody wallets, including private keys and

seed phrases. The Company cannot control or secure data processed by Third-Party Services, including, but not limited to external wallet providers, network infrastructure, or public blockchain environments.

8.3 Data Breach Notification**.** If an incident occurs that leads to the unauthorized access, disclosure, alteration, or loss of Personal Data, and the Company determines that the breach presents a real risk of harm to affected individuals, we will notify the relevant authority in the British Virgin Islands and the affected Users as soon as reasonably practicable. Such notification will include the nature of the breach, the potential impact, and the measures taken or proposed to mitigate any adverse effects.

9. DATA RETENTION

9.1 We retain Personal Data only for as long as it is necessary to fulfill the purposes for which it was collected or as required by applicable law. Retention periods depend on the type of data and the legal basis for its Processing.

9.2 Personal Data related to your Account is generally kept for the duration of your use of the Emyo Services and for a reasonable period after account closure, to comply with legal, regulatory, and operational requirements. Information collected for KYC/AML compliance may be retained for the period required under applicable AML and sanctions regulations. Technical logs, security data, and transactional information may be stored for periods necessary to maintain platform security, investigate potential misuse, or meet regulatory or audit obligations.

9.3 Marketing-related data and cookie-based identifiers are retained only until you withdraw your consent or disable such technologies. After consent is withdrawn, we stop Processing such data for marketing purposes, and related data is either deleted or anonymized, unless retention is required for legitimate security, audit, or compliance reasons.

9.4 Where longer retention is required to comply with a legal obligation, resolve disputes, prevent fraud, or establish or defend legal claims, we may retain relevant Personal Data for as long as necessary for those purposes.

9.5 Once the applicable retention period expires, Personal Data is securely deleted or irreversibly anonymized in accordance with the Company's internal procedures and applicable legal requirements.

9.6 Waitlist data is retained only for as long as necessary to: administer the Waitlist and Token Sale processes, comply with applicable legal and regulatory requirements, or maintain accurate records to prevent fraud or unauthorized activity. Where consent is withdrawn or where the data is no longer required for Waitlist purposes, it will be deleted or anonymized unless retention is required by law or legitimate business needs.

10. CHILDREN'S PERSONAL INFORMATION

10.1 The Website and Services are not directed to persons under the age of 18, and we do not knowingly collect Personal Data from anyone under this age. If we have reason to believe that a User is under 18, the User's Account will be suspended or closed, and the individual will not be permitted to continue using the Emyo Services. We will delete any associated Personal Data as soon as reasonably practicable, unless retention is required for compliance or investigation purposes.

10.2 If you become aware of any person under the age of 18 using the Emyo Services, please notify us so that we can take appropriate action.

11. CROSS BORDER DATA TRANSFERS

11.1 We may transfer or store Personal Data outside the British Virgin Islands when this is necessary for the operation of the Emyo Services, including the use of hosting providers, technical infrastructure, KYC/AML providers, analytics tools, or other Third-Party Services located in other jurisdictions.

11.2 When such transfers occur, we ensure that the receiving parties are subject to appropriate contractual, technical, or organizational safeguards designed to protect Personal Data in accordance with the requirements of the BVI Data Protection Act, 2021.

11.3 By using the Emyo Services, you acknowledge that certain data may be processed in countries that may have different data-protection standards than those in your jurisdiction.

11.4 **Blockchain Transfer Notice**. Certain interactions with Tokens occur on public blockchain networks. Public blockchains are decentralized and operate across multiple jurisdictions, meaning that on-chain data (including Wallet Addresses, transaction hashes, timestamps, staking activity, and smart-contract interactions) may be processed globally the moment a transaction is broadcast. Because blockchain networks are publicly accessible and not controlled by the Company, any data recorded on-chain may be viewed, accessed, or stored by parties in various jurisdictions outside the Company's control. Such transfers are inherent to blockchain technology and occur automatically as part of network validation and transaction processing. By using the Emyo Services and interacting with blockchain components, you acknowledge that on-chain data may be transferred internationally, may become permanently publicly available, and cannot be altered, restricted, or deleted by the Company once written to the blockchain.

12. USER RIGHTS AND OBLIGATIONS

12.1 User Rights

(a) Users may request access to the Personal Data the Company holds about them;

(b) Users may request correction of inaccurate or incomplete Personal Data;

(c) Users may request deletion of Personal Data where it is no longer required for the purposes for which it was collected and where retention is not required by law or legitimate business needs. Certain categories of data cannot be deleted, including:

- **(i)** KYC/AML records required by applicable regulations;
- **(ii)** transaction logs necessary for compliance, security, or audits;
- **(iii)** information stored on public blockchains, which is technically immutable and outside the Company's control.

(d) Users may object to or request restriction of Processing based on legitimate interests, unless the Company has overriding lawful grounds, or the Processing is necessary for compliance, security, or fraud-prevention purposes;

(e) Users may withdraw previously given consent at any time. Withdrawal does not affect lawful Processing performed prior to withdrawal;

(f) Users have the right to bring a claim before the competent data protection Supervisory Authority.

(g) requests may be submitted using the contact details provided in this Policy. The Company may take reasonable steps to verify identity and may decline requests where permitted or required by applicable law.

12.2 User Obligations

(a) users must ensure that all Personal Data provided during registration, KYC, or use of the Services is accurate, complete, and up to date;

(b) users must comply with applicable KYC/AML requirements, eligibility rules, geographic restrictions, and platform policies;

(c) users are responsible for the security of their devices, networks, Wallet Addresses, and private keys. The Company cannot recover or secure private keys, seed phrases, or self-custody wallet data;

(d) users must not engage in fraudulent, abusive, deceptive, or unlawful activities, attempt to bypass restrictions, misuse the Services, or interfere with platform integrity;

(e) users must cooperate with the Company in connection with compliance checks, identity verification, fraud investigations, or security reviews where required by law or platform policies.

13. COOKIES

13.1 The Website may use cookies and similar technologies to operate, secure, and improve the Emyo Services. The use of cookies, the types we use, and your options for managing them are described in our separate Cookie Policy, which is available on the Website.

14. USER REQUEST PROCEDURE

14.1 Users may exercise their rights regarding Personal Data by submitting a request to the Company by contacting the Company at the email address: legal@emyo.io. The Company will review and respond to such requests within a reasonable period, taking into account the nature and complexity of the request and applicable legal obligations.

14.2 To protect Personal Data, the Company may require Users to verify their identity before processing a request. Verification may include confirming Account details, Wallet Address associations, or providing identification information where necessary. Any data collected for verification will be used solely for this purpose.

14.3 The Company may decline a request where required by law, where the User cannot be reliably identified, where the request concerns information that cannot be deleted for compliance, security, or fraud-prevention reasons, or where the data is stored on public blockchain networks and cannot be altered or removed. The Company may also refuse requests that are manifestly unfounded or excessive. Where a request is denied, the Company will inform the User of the reason unless restricted by law or security considerations.

14.4 Submitting a request does not require payment, unless repeated or unreasonable requests impose administrative burdens, in which case the Company may charge a reasonable fee or decline further processing as permitted by applicable law.

14.5 Users who have concerns about the handling of their Personal Data are encouraged to contact the Company so that the matter can be addressed promptly.

15. CHANGES TO THE POLICY

15.1 The Company may update or modify this Privacy Policy from time to time to reflect changes in legal requirements, operational needs, or the functionality of the Emyo Services. Any updates will be posted on the Website, and the revised Policy will become effective upon publication unless otherwise stated. Your continued use of the Emyo Services after any changes to this Policy constitutes your

acknowledgment of the updated version. Users are encouraged to review this Policy periodically to stay informed about how Personal Data is processed.

15.2 If the Company makes material changes that significantly affect how Personal Data is processed, we may provide an additional notice through the Website or other appropriate means. Such notice does not waive or modify any disclaimers or eligibility restrictions applicable to the Emyo Services.

16. GOVERNING LAW AND JURISDICTION

16.1 **Governing law.** This Privacy Policy, and any non-contractual obligations arising out of or in connection with it, are governed by and shall be construed in accordance with the laws of the British Virgin Islands, without giving effect to any choice-of-law or conflict-of-laws rules that would result in the application of the laws of any other jurisdiction.

16.2 **Arbitration.** Any dispute, controversy, or claim arising out of or in connection with this Privacy Policy or the processing of your Personal Data shall be finally resolved by arbitration under the Rules of the BVI International Arbitration Centre ("BVI IAC"), which rules are deemed to be incorporated by reference into this clause. The arbitral tribunal shall consist of one (1) arbitrator, the seat (legal place) of arbitration shall be Road Town, Tortola, British Virgin Islands, and the language of the arbitration shall be English.

16.3 **Waiver of class actions and jury trials.** To the fullest extent permitted by applicable law, you and the Company agree that: (a) any arbitration shall be conducted only on an individual basis and not as a class, collective, representative, or group proceeding; and (b) you and the Company each irrevocably waive any right to a trial by jury or to participate as a plaintiff or class member in any purported class, collective, or representative proceeding relating to any dispute arising out of or in connection with this Privacy Policy.

17. CONTACT INFORMATION

17.1 If you have questions about this Privacy Policy or wish to submit a request regarding your Personal Data, you may contact the Company using the following address:

ToyCarma Inc. (mailing address): 30 N Gould St Ste 12607, Sheridan, WY 82801
Contact email:legal@emyo.io

17.2 The Company will make reasonable efforts to review and respond to inquiries in accordance with applicable law and internal procedures.