

PRIVACY POLICY

CLOCK IN – A SOLANA MOBILE HACKATHON

Effective Date: 3 September 2026

This Privacy Policy ("Policy") explains how Radiants DAO Ltd., incorporated in the British Virgin Islands ("Radiants DAO", "Organizer", "we", "us" or "our"), collects, uses, stores, discloses and otherwise processes personal data in connection with Clock In - A Solana Mobile Hackathon (the "Hackathon"), the official Hackathon website at <https://solanamobile.radiant.nexus/> (the "Official Website"), participant registration, fixed team rosters, submissions, judging, Finalist verification, designated Team Representatives and prize administration.

This Policy should be read together with the Hackathon Terms and Conditions (the "Terms"). Capitalized terms not defined in this Policy have the meanings given to them in the Terms. If a third-party service used for the Hackathon, including Sumsb, has its own privacy notice, that notice also applies to the processing carried out independently by that third party. This Policy governs the Organizer's processing and does not replace a third party's own legally required disclosures.

1. DATA CONTROLLER

Radiants DAO Ltd. is the data controller for personal data that it determines how and why to process in connection with the Hackathon. The Organizer may engage data processors and service providers to process personal data on its behalf. For mandatory Finalist identity and compliance verification, the Organizer currently intends to use Sumsb, or another reputable verification provider designated in accordance with the Terms.

Privacy contact: hackathon@radiant.nexus. You may use this address for privacy questions, data-rights requests, or complaints concerning the Organizer's handling of your personal data.

2. SCOPE

This Policy applies to personal data relating to individuals who visit or interact with the Official Website, register for or participate in the Hackathon, contribute to a team, are recorded on a fixed team roster, act as a Team Representative, submit a Project, communicate with the Organizer, act as a Finalist or prize recipient, or otherwise interact with the Hackathon. It also applies where the Organizer receives personal data about a participant from a teammate, Team Representative, judge, sponsor, verification provider, service provider, public source or competent authority.

The Hackathon is intended for adults who meet the eligibility requirements in the Terms. It is not intended for children. We do not knowingly invite or permit participation by persons under 18 years of age or below the age of legal majority applicable to them where that age is higher.

3. PERSONAL DATA WE MAY COLLECT

3.1 Registration and Contact Data

We may collect your name, username or handle, email address, country of residence, team name, team role, team-member details, designation as the Team Representative, communications preferences, representative instructions or authority confirmations, and other information you provide when registering, joining a team, contacting us, or participating in Hackathon activities.

3.2 Eligibility and Participation Data

We may collect information reasonably necessary to assess eligibility under the Terms, including age or age confirmation, country of residence, project start date, team composition, the fixed team roster recorded at the Submission Time, submission timestamps, any permitted clerical or administrative correction to the roster, prior funding status, representations concerning venture capital or angel funding, and information relevant to sanctions, restricted-jurisdiction, conflict-of-interest, KYC/AML, or other participation requirements.

3.3 Project and Submission Data

We may collect or access Project titles, descriptions, GitHub repository information, source-code links, Android APKs or build information, demo videos, pitch decks, presentation materials, screenshots, technical documentation, Solana addresses or program identifiers, Mobile Wallet Adapter or Solana Mobile Stack integration information, authorship information, and other materials submitted for judging or technical verification. Submission materials may contain personal data about team members or other persons.

Submissions are not made or received in confidence under the Terms. This Policy does not convert submission materials into confidential information or create a confidentiality obligation beyond the Organizer's obligations with respect to personal data under applicable law. Participants should not include trade secrets, confidential or commercially sensitive information, passwords, credentials, private keys, seed phrases, unnecessary sensitive or biometric data, or third-party personal data that is not reasonably necessary for the Hackathon. Participants are responsible for having a lawful basis and any necessary authority to include personal data relating to another person in a submission.

3.4 Judging and Administrative Data

We may process numerical scores, judge comments, rankings, provisional Finalist or winner selections, eligibility and compliance assessments, technical-review findings, communications with judges or participants, disqualification records, winner status, publication status on the Solana dApp Store, and records needed to administer deadlines, prize decisions, corrections permitted under the Terms, or Hackathon operations. Scores and rankings may be treated as provisional until the Organizer completes applicable eligibility, technical, KYC/AML, sanctions, funding-status, tax and prize-payment checks.

3.5 Prize and Wallet Data

Where relevant to a prize, we may collect the identity and designation of the Team Representative, the Nominated Prize Wallet supplied or confirmed by that representative, wallet-verification information, written payment instructions or confirmations, transaction hashes and transfer records, tax or reporting information, prize-selection records, and information reasonably necessary to deliver, document, withhold, forfeit, reallocate or otherwise administer a prize. The Nominated Prize Wallet and an on-chain prize transaction may be publicly visible. We do not require or ask for private keys, seed phrases, or wallet passwords.

3.6 Team Representative and Internal Dispute Data

We may process the Team Representative's designation, authority confirmations, team-level instructions, replacement requests, communications and records of any dispute raised by a participant concerning prize sharing, ownership, equity, revenue, contribution, compensation or related team matters. We process such information only to the extent reasonably necessary to administer the Hackathon, determine whether prize payment can lawfully and safely proceed, preserve an accurate record, comply with binding legal process, or establish, exercise or defend legal rights. The Organizer does not undertake to investigate or adjudicate the merits of internal team disputes. Participants should not send us sensitive, confidential or unrelated information merely to support an internal team dispute.

3.7 Website, Device and Technical Data

When you use the Official Website or related services, we or our providers may receive technical information such as IP address, browser type, operating system, device identifiers or characteristics, timestamps, referral information, pages or features used, approximate location derived from IP address, logs, error information, and security or anti-fraud signals. The exact data depends on the technology and service providers used on the Official Website.

3.8 Communications and Support Data

We may retain emails, messages, support requests, feedback, complaints, questions, and records of our communications with you where reasonably necessary to administer the Hackathon, resolve issues, maintain records, or protect legal rights.

4. FINALIST KYC / AML AND IDENTITY VERIFICATION

4.1 Mandatory Verification

As stated in the Terms, each individual participant recorded on the fixed team roster of a Finalist team at the Submission Time must complete identity verification and KYC/AML and sanctions screening through Sumsub, or another verification provider designated by the Organizer, within the notified deadline. A team may not remove, replace or disregard a rostered member after the Submission Time to avoid that person's verification requirement. Successful completion of all required individual verifications is a condition to confirmation of Finalist status and to the team's receipt of any prize, and the Organizer may withhold the entire team's prize where a required team member does not satisfactorily complete verification in accordance with the Terms.

4.2 Verification Data

Depending on the verification checks configured by the Organizer and permitted by applicable law, the verification provider may collect and process: full name; date and place of birth; nationality; residential or current address; email address or phone number; government-issued identification document type, number, issuing country, expiry date, machine-readable-zone data, barcodes and document images; photographs or scans of the face; selfies; video or liveness recordings; facial features or other biometric-derived data used for identity matching; IP address, device and fraud-prevention signals; sanctions, politically exposed person (PEP), watchlist and adverse-media screening results; and additional supporting information needed to resolve an identity, fraud or compliance question.

4.3 Role of Sumsub

Where Sumsb processes personal data to perform verification steps configured by the Organizer, Sumsb acts as a processor on the Organizer's instructions for those service-delivery activities. Sumsb may also act as an independent controller for limited processing undertaken for its own lawful purposes, legal obligations, service development, security or fraud-prevention activities, as described in its applicable privacy notices. Sumsb's service privacy notice is available at <https://sumsub.com/privacy-notice-service/>.

4.4 Biometric Data and Separate Consent

Identity verification may use facial-image comparison, liveness checks, or biometric-derived facial features to confirm that a person presenting an identity document is the same person shown in that document and to detect impersonation or fraud. Before personal data is transferred to or collected through Sumsb or another verification provider, the Organizer will provide, or ensure that the verification flow provides, any notices and obtains any consents required by applicable law for the configured checks. Where applicable law requires specific, written, informed, or separate consent for biometric processing, that consent will be requested before the relevant biometric processing occurs. A person who does not complete legally required verification may be unable to be confirmed as a Finalist or receive a prize, subject to any rights or alternatives required by applicable law.

4.5 Verification Outcomes

The Organizer may receive verification status, risk indicators, screening results, supporting information, or other information necessary to determine whether verification has been completed and whether an unresolved legal, sanctions, fraud or compliance risk exists. The Organizer will seek to receive no more raw identity or biometric material than reasonably necessary for Hackathon purposes. Where reasonably practicable, the Organizer may request further information or permit manual review before making a final adverse eligibility decision. We do not intend to make a Finalist or prize decision solely on the basis of an automated score where applicable law requires meaningful human involvement or review. If any required member of a fixed Finalist roster does not satisfactorily complete verification, the resulting team-level consequences - including withholding, forfeiture or reallocation of the entire team's prize - will be administered in accordance with the Terms.

5. HOW WE USE PERSONAL DATA

We may process personal data for the following purposes:

to register participants, create or administer teams, record and preserve the fixed team roster at the Submission Time, identify the Team Representative, confirm eligibility, and communicate Hackathon rules, deadlines and operational information;

to receive, host, access, disclose as permitted by the Terms, review, test and evaluate submissions and to facilitate judging and technical verification, recognizing that submissions are not made in confidence;

to verify compliance with project-age, mobile-development, funding-status, country, sanctions, identity, KYC/AML, anti-fraud and other eligibility requirements;

to calculate and record scores and provisional rankings, select, announce and verify Finalists and winners, complete eligibility and compliance checks before any prize entitlement is confirmed, administer prizes through the Team Representative, verify the Nominated Prize Wallet and payment instructions, maintain transfer and discharge records, and comply with tax or reporting obligations where applicable;

to process team-level communications and internal dispute information to determine whether Hackathon administration or prize payment can proceed, preserve evidence of instructions and payment, comply with binding legal process, and protect the Organizer's legal rights, without undertaking to adjudicate internal ownership, equity, revenue or prize-sharing disputes;

to confirm the publication of winning applications to the Solana dApp Store where required by the Terms;

to prevent cheating, plagiarism, duplicate participation, post-submission roster manipulation, identity substitution, manipulation, malware, sanctions evasion, fraud, abuse, security incidents or unlawful conduct;

to communicate with participants, answer questions, manage complaints, investigate rule violations, and enforce the Terms;

to operate, secure, troubleshoot, maintain and improve the Official Website and Hackathon infrastructure;

to create Hackathon records, statistics and internal analytics, including aggregated or de-identified information where appropriate;

to publicize and archive the Hackathon, including identifying Finalists and winners and using submitted materials in accordance with the license and publicity provisions in the Terms;

to comply with applicable law, sanctions requirements, court orders, regulatory or law-enforcement requests, and to establish, exercise or defend legal claims; and

to carry out any other compatible purpose disclosed to you at the time of collection or otherwise permitted by applicable law.

6. LEGAL BASES AND CONDITIONS FOR PROCESSING

The lawful basis or legal condition relied upon depends on the applicable law and the specific processing activity. Where the BVI Data Protection Act, 2021 (the "BVI DPA") applies, personal data will be processed on the basis of express consent unless a condition permitted by the BVI DPA applies, including where processing is necessary for performance of the Terms or steps requested before participation, compliance with a legal obligation, protection of vital interests, administration of justice, or exercise of a function conferred by law. In all cases, the Organizer will seek to process personal data for a lawful Hackathon-related purpose, only to the extent necessary or directly related to that purpose, and in a manner that is adequate and not excessive. Where another law such as the EU GDPR or UK GDPR applies, additional lawful bases may be available, including legitimate interests where that law permits their use.

Where personal data is considered sensitive, special-category, biometric or otherwise specially protected under applicable law, we will rely on the additional condition required by that law. Depending on the applicable regime and processing activity, this may include explicit consent, a legally recognized compliance or public-interest condition, fraud-prevention grounds, establishment or defence of legal claims, or another legally available condition. Consent may be withdrawn where processing is based on consent, but withdrawal does not affect processing already lawfully undertaken and may affect a participant's ability to complete a verification step, remain eligible, or receive a prize where the relevant data is necessary and no alternative lawful basis or verification method is available.

7. SOURCES OF PERSONAL DATA

We may obtain personal data directly from you; from your teammates, Team Representative or other authorized representative; from the fixed team roster and submission records; from Project materials and public blockchain records; from judges, sponsors and Hackathon partners; from Sumsb and other service providers; from public or commercially available sanctions, PEP, watchlist, adverse-media, company, professional or fraud-prevention sources; from the Solana dApp Store or related ecosystem services where necessary to verify publication; and from governmental, regulatory, court or arbitral authorities where lawful.

If you provide personal data about another person, including a teammate, prize-wallet owner or other individual, you must have authority or another lawful basis to provide that information and must not provide more information than reasonably necessary. Where appropriate, you should direct that person to this Policy. A Team Representative who provides a Nominated Prize Wallet or team-level instruction is responsible under the Terms for having authority to provide that instruction on behalf of the team.

8. DISCLOSURE AND SHARING OF PERSONAL DATA

We may disclose personal data only where reasonably necessary for the purposes described in this Policy, including to:

Sumsb or another designated identity, KYC/AML, sanctions, fraud-prevention or compliance provider;

cloud hosting, website, communications, analytics, security, form, file-storage, developer-tooling, payment, wallet-verification, tax or operational service providers;

judges, reviewers and technical evaluators to the extent reasonably necessary to evaluate submissions, conduct technical review and administer judging, including submission materials that are not treated as confidential under the Terms;

Hackathon sponsors and partners where reasonably necessary to deliver a prize, device, benefit or program function, administer the Hackathon, or where you have otherwise been appropriately informed of the disclosure;

the Team Representative and, where necessary, other members of the same team for team-level administration or prize processing; however, we will not ordinarily disclose another participant's underlying identity documents, biometric material, detailed screening results or unrelated KYC information to teammates and may instead communicate only the minimum status information reasonably necessary;

professional advisers, including lawyers, accountants, auditors, insurers and compliance consultants;

competent courts, regulators, law-enforcement bodies, sanctions authorities, tax authorities or other public authorities where disclosure is required or legally justified;

a successor, purchaser, investor or transaction counterparty in connection with a bona fide restructuring, merger, sale, financing or transfer involving the Organizer, subject to appropriate confidentiality and data-protection safeguards; and

other persons where you direct or authorize the disclosure or where disclosure is otherwise permitted by applicable law.

We do not sell participant identity documents or biometric data. We do not authorize service providers to use participant personal data for their own unrelated marketing merely because they process data for the Hackathon.

9. PUBLIC INFORMATION, WINNER ANNOUNCEMENTS AND BLOCKCHAIN DATA

The Hackathon is a public technology competition. Information that you intentionally publish in a public GitHub repository, demo video, pitch presentation, social-media post, public blockchain transaction, Solana program, Solana dApp Store listing, or other public channel may be accessible globally and may be copied or indexed by third parties outside the Organizer's control.

The fact that submissions are not made in confidence does not mean that every submission or every item of personal data will automatically be published to the general public. It means that, subject to applicable data protection law and the Terms, submission materials may be disclosed to and used by the Organizer, judges, technical reviewers, service providers and relevant sponsors or partners for Hackathon administration, judging, verification, archival, publicity and marketing purposes. Participants should therefore exclude trade secrets and other information they do not wish to disclose to those recipients.

We may publicly announce or display the names, team names, Project names, descriptions, images, demo materials, rankings, finalist or winner status, prize category and other reasonable publicity information relating to Finalists and winners, consistent with the Terms and applicable law. We will not publish government identity documents, KYC files, private verification records, or non-public biometric data as part of winner announcements.

Public blockchains are designed to maintain persistent records. If a prize is delivered to the Nominated Prize Wallet, the wallet address, transaction hash, amount and related on-chain information may remain publicly visible and may not be capable of deletion by the Organizer. The Organizer may also retain off-chain records showing the Team Representative's confirmed wallet instruction and completion of the transfer for audit, dispute and legal-claims purposes.

10. COOKIES, ANALYTICS AND SIMILAR TECHNOLOGIES

The Official Website may use cookies, local storage, pixels, logs or similar technologies that are strictly necessary for operation, security, fraud prevention, preferences, performance or analytics. Where applicable law requires consent for non-essential cookies or similar technologies, we will request that consent through an appropriate mechanism before using them. The particular cookies and providers in use may change as the Official Website is maintained; any dedicated cookie notice or consent interface displayed on the Official Website forms part of our privacy disclosures.

11. INTERNATIONAL DATA TRANSFERS

The Hackathon is international and participants may be located in many countries. Personal data may therefore be accessed, processed or stored outside your country of residence, including in the British Virgin Islands, the United Kingdom, the European Economic Area, the United States, and jurisdictions in which our service providers or their subprocessors operate.

Where applicable data protection law restricts international transfers, we will use a legally recognized transfer mechanism or other appropriate safeguard where required. In particular, where the BVI DPA

applies, the Organizer will transfer personal data outside the British Virgin Islands only where the transfer is supported by adequate data-protection safeguards or the data subject's consent, as required by that Act. Under other applicable regimes, safeguards may include adequacy findings, contractual safeguards, consent where legally valid, or another permitted transfer basis. Sumsb describes its international-transfer safeguards in its applicable privacy notices. No method of international transfer or storage can eliminate all risk, but we and our providers are expected to apply safeguards appropriate to the nature of the data and applicable law.

12. DATA RETENTION

We retain personal data only for as long as reasonably necessary for the purposes for which it was collected, including Hackathon administration, prize delivery, compliance, fraud prevention, dispute resolution, audit, accounting, tax, security and legal-claims purposes, and for any additional period required or permitted by applicable law.

As a general working schedule, ordinary registration, participation, judging and Hackathon-administration records may be retained for up to three (3) years after the Hackathon concludes, unless a shorter period is appropriate or a longer period is reasonably necessary for a dispute, investigation, legal obligation, audit or enforcement of the Terms. Prize, Team Representative, Nominated Prize Wallet, payment-instruction, transfer, tax, sanctions, fraud, internal-dispute or Finalist compliance records may be retained for up to five (5) years after the relevant verification or prize event, or longer where required by law or reasonably necessary for a continuing legal claim, investigation, compliance matter or binding legal process.

The Organizer will seek to minimize its possession of raw identity documents and biometric verification material. Where Sumsb or another provider collects such material directly, retention and deletion within that provider's systems are governed by the Organizer's documented instructions, the provider's applicable contractual and legal obligations, and applicable law. Sumsb states that client-controlled verification data is retained according to client instructions and applicable legal requirements, with specific jurisdictional rules potentially applying to biometric data. Participants should review Sumsb's current service privacy notice for further detail.

We may retain de-identified or aggregated information that no longer identifies an individual for longer periods where lawful. Public blockchain data and information independently published by you or by third parties may remain available indefinitely and may be outside our ability to erase.

13. SECURITY

We use reasonable administrative, technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access, misuse or other unlawful processing. Measures may include access controls, role-based permissions, secure service providers, authentication, logging, encryption in transit or at rest where appropriate, vendor due diligence, data minimization and incident-response procedures.

No website, network, blockchain, cloud platform or verification system is completely secure. Participants are responsible for protecting their own devices, accounts, authentication credentials and wallets and must never send us a private key, seed phrase, or wallet password.

14. YOUR PRIVACY RIGHTS

Depending on your location and the law applicable to the processing, you may have rights concerning your personal data. These may include rights to request access to personal data we hold about you; request correction of inaccurate or incomplete data; request deletion or restriction in circumstances provided by law; object to certain processing; withdraw consent where consent is the basis for processing; obtain certain data in a portable format where applicable; opt out of certain marketing, sale, sharing or targeted-advertising activities where applicable; request information about categories of data and recipients; and complain to a competent data-protection or supervisory authority.

Rights are not absolute. We may need to verify your identity before acting on a request and may decline or limit a request where permitted by law, including where retention is required for compliance, fraud prevention, security, tax, legal claims, the rights of others, or preservation of an accurate historical record. A right to correct inaccurate personal data does not ordinarily require the Organizer to rewrite a record that accurately reflects the fixed team roster, Team Representative designation or prize instruction as it existed at the relevant time; where appropriate, we may correct the inaccurate data, add a supplementary notation, or preserve both the original record and the correction. Exercising a legally protected privacy right will not itself result in discrimination or disqualification, although deletion, withdrawal of consent or restriction may affect eligibility or prize processing where the relevant data is necessary and no alternative lawful basis or verification method is available.

To exercise a right concerning the Organizer's processing, contact hackathon@radiant.nexus. If your request concerns data held by Sumsb as part of your verification, you may contact the Organizer first because the Organizer controls the verification process for Hackathon purposes. Sumsb also provides data-subject-rights information through its Privacy Hub at <https://sumsub.com/privacy-notice/>.

15. U.S. STATE PRIVACY AND BIOMETRIC NOTICES

Participants residing in the United States may have additional rights under applicable state privacy or biometric laws. Where such a law applies, this Section supplements the remainder of the Policy and the more protective applicable requirement will govern to the extent of a conflict.

If biometric identity verification is required for a U.S. participant in a jurisdiction that requires written disclosure and consent, including where applicable Illinois, Washington or Texas, the verification flow will provide or link to the required biometric disclosure and obtain the legally required affirmative consent before the covered biometric data is processed. Biometric data used for Hackathon verification is intended for identity matching, liveness, authentication, fraud prevention and related compliance purposes, not for sale or unrelated advertising. The Organizer does not sell, lease or trade biometric data.

Retention and destruction of biometric data will follow applicable law, the Organizer's instructions to the verification provider, and the provider's legally applicable retention schedule. Sumsb publishes a separate biometric acknowledgement and consent for relevant services and describes jurisdiction-specific retention and destruction terms in its privacy materials. If a state law grants an appeal or opt-out right that applies to our processing, requests may be submitted to hackathon@radiant.nexus.

16. EEA, UNITED KINGDOM AND OTHER REGULATED-JURISDICTION PARTICIPANTS

Where the EU General Data Protection Regulation, UK GDPR, or another data protection regime applies to particular processing, we will apply the additional rights, transparency, lawful-basis, sensitive-data, processor-contracting, security and international-transfer requirements applicable to that processing. References in this Policy to legitimate interests, consent, contractual necessity, legal obligation and special-category or biometric conditions are intended to operate only to the extent recognized by the law that applies.

Participants may contact the competent supervisory authority in their jurisdiction where they believe their data-protection rights have been infringed. We encourage participants to contact us first where appropriate so we can review and address the concern.

Where an applicable data-protection regime requires the Organizer to appoint a local representative, the Organizer will make the representative's required contact details available through the Official Website or another appropriate Hackathon privacy notice.

17. MARKETING COMMUNICATIONS

We may send operational Hackathon communications where necessary to administer your participation. Promotional or marketing communications will be sent only where permitted by applicable law and, where required, with consent. You may opt out of non-essential marketing communications using the unsubscribe mechanism provided or by contacting us. Opting out of marketing does not prevent us from sending important administrative, compliance, security, prize or legal notices connected with the Hackathon.

18. THIRD-PARTY SERVICES AND LINKS

The Official Website, submissions or Hackathon communications may link to or integrate third-party websites or services, including GitHub, video-hosting services, the Solana ecosystem, wallet providers, the Solana dApp Store, Sumsb, sponsors or other providers. Those third parties may process personal data under their own terms and privacy notices and, depending on the activity, may act as processors for the Organizer or as independent controllers for their own purposes. We are not responsible for independent third-party privacy practices, and participants should review the relevant notices before providing information or using those services.

19. DATA BREACHES AND INCIDENTS

If we become aware of a personal-data breach affecting Hackathon data, we will investigate and take reasonable containment and remediation steps. Where applicable law requires notification to affected individuals, regulators or other authorities, we will provide notification in the manner and timeframe required by that law. We may also require participants to cooperate with reasonable security steps where an incident relates to a participant account, submission, wallet, device or communication channel.

20. CHANGES TO THIS POLICY

We may amend this Policy where reasonably necessary to reflect changes to the Hackathon, the Terms, service providers, verification methods, prize administration, technology, legal requirements or our data-processing practices. The current version will be made available through the Official Website or another official Hackathon channel. Where a change materially affects how already-collected personal data is used,

we will provide additional notice, obtain consent, or take another step where required by applicable law. A change to this Policy does not by itself create a new right to alter the fixed team roster or otherwise override the Terms.

21. CONTACT AND COMPLAINTS

Controller: Radiants DAO Ltd., British Virgin Islands

Official Website: <https://solanamobile.radiant.nexus/>

Privacy and Hackathon Contact: hackathon@radiant.nexus