Privacy Policy

Effective Date: 15th July 2025

Last Updated: 15th July 2025

East Emblem Ltd ("East Emblem", "we", "us", or "our") operates the Second Chance platform, a founder evaluation and investor-matching tool that uses both human and algorithmic inputs to analyze startup submissions and investor preferences.

East Emblem is a company registered in Masdar City Free Zone, Abu Dhabi, under license number MC 13353, with its principal place of business at Smart Station, First Floor, Incubator Building, Masdar City, Abu Dhabi, United Arab Emirates.

This Privacy Policy explains how we collect, use, store, share, and protect your Personal Data when you engage with Second Chance, whether as a founder, investor, partner, contractor, or site visitor. It also outlines your rights under UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and other applicable regulations (such as GDPR where relevant), and how you may exercise those rights.
This policy applies to:

- Visitors to our websites and digital platforms
- Registered users and platform participants (e.g., founders, investors, analysts)
- Recipients of our communications and marketing content
- Business partners, service providers, and advisors
- Any individual whose personal data is collected, received, or processed by East Emblem

By using our platform, submitting information, or engaging with us, you agree to the practices described in this policy.

If you do not agree with this policy, you should discontinue use of our services and contact us at info@eastemblem.com with any concerns.

2: Definitions

In this Privacy Policy, the following terms shall have the meanings set out below:

"Personal Data" Any data relating to an identified or identifiable natural person ("Data Subject"), whether directly or indirectly. This includes, but is not limited to: names, email addresses, phone numbers, job titles, device identifiers, IP addresses, startup-related submissions, investor profiles, and online behavioral data.

"Processing" Any operation or set of operations performed on Personal Data, whether by automated means or not. This includes collection, recording, storage, use, analysis, modification, transfer, disclosure, publication, restriction, erasure, or destruction of Personal Data.

"Special Category Data" Personal Data that is sensitive in nature and requires enhanced protection, including data relating to racial or ethnic origin, health status, biometric or genetic data, religious beliefs, political opinions, or criminal records. East Emblem does not knowingly collect Special Category Data unless explicitly required and permitted by applicable law.

"Data Controller" The person or entity that determines the purposes and means of Processing Personal Data. For most Processing activities described in this Policy, East Emblem Ltd acts as the Data Controller.

"Data Processor" Any third party who processes Personal Data on behalf of the Data Controller and under its instructions, such as IT vendors, cloud service providers, analytics platforms, and subcontracted consultants.

"Data Subject" An individual whose Personal Data is collected, stored, or processed by East Emblem. This includes founders, investors, partners, employees, contractors, and users of the Second Chance platform.

"UAE PDPL" The Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, applicable throughout the United Arab Emirates, which governs the lawful Processing of Personal Data and defines the rights of Data Subjects and obligations of Controllers and Processors.

"AI System" or "Automated Processing" Any system or functionality that uses algorithmic or artificial intelligence techniques to analyze or process Personal Data, including startup scoring, proof assessment, and investor-match routing on the Second Chance platform.

"Standard Contractual Clauses (SCCs)" Legally recognized data protection safeguards used in international data transfers to jurisdictions that do not offer adequate protection under applicable law.

"Consent" Any clear and affirmative action that indicates the Data Subject's agreement to the Processing of their Personal Data for specified purposes. Consent may be withdrawn at any time.

3: What Data We Collect

East Emblem Ltd collects various categories of Personal Data through the Second Chance platform and related digital services. We collect this information directly from you, automatically through your device, or from third parties, as outlined below.

3.1 Information You Provide to Us

We collect Personal Data that you submit directly through our platform, via forms, uploads, emails, live sessions, applications, surveys, and onboarding calls. This may include:

A. Founder & Startup Information

- Full name, email address, mobile number
- Nationality, location, and time zone
- Company name, legal structure, registration details
- Pitch decks, business models, investor decks, and traction updates
- Founder profile information (CVs, LinkedIn, prior experience)
- Video recordings, submitted statements, and application narratives
- Financial projections and funding history

B. Investor and Partner Information

- Full name, professional affiliation, contact details
- Investor mandate, ticket size, stage/sector focus
- Custom intake notes, discovery calls, and matching preferences

C. Communications and Support Data

- Records of email exchanges, helpdesk messages, and call logs
- Webinar registrations, survey responses, and workshop attendance

3.2 Information We Collect Automatically

When you interact with our platform, we automatically collect certain technical and behavioral data using cookies, tracking pixels, analytics tools, and log files:

- IP address and location data (based on device or browser)
- Device type, operating system, browser, and screen resolution
- Login timestamps and session duration
- Clickstream data, navigation paths, scroll depth, and engagement heatmaps
- Cookie identifiers and unique session tokens
- Behavior within founder dashboards or investor viewports (e.g. which profiles you view or shortlist)

This data helps us personalize the platform experience, optimize usability, and improve investor-founder matching outcomes.

3.3 Data from Third Parties or Integrated Services

We may receive limited Personal Data about you from third-party sources or services you connect to Second Chance, including:

- LinkedIn or Google login credentials (if used for authentication)
- Event registration platforms (e.g. if you attended one of our affiliated demo days)
- Partner accelerators, fund managers, or institutional sponsors who refer you to the platform

Where applicable, we will ensure such third parties have a lawful basis to share your data with us.

3.4 Special Category Data
We do not actively request or process Special Category Data (such as health status, biometric data, religion, or political affiliation). If you voluntarily submit such data (e.g., in a video pitch or deck), it is done at your discretion and will not be used as part of automated scoring unless required by law or necessary for specific services (e.g., demographic data for impact funders).

3.5 Aggregated and Anonymized Data
We may aggregate and anonymize Personal Data for analytical, benchmarking, or research purposes. Such data will no longer be identifiable and is therefore not considered Personal Data under this Policy.

4: How and Why We Process Personal Data
We collect and process Personal Data to operate and improve the Second Chance platform, provide services to our users, fulfill our legal and contractual obligations, and pursue legitimate business interests. Our use of your data is guided by principles of necessity, transparency, and proportionality. All processing activities are based on a clear legal basis and are aligned with the expectations of users, partners, and regulators.

One of the primary reasons we process Personal Data is to deliver the core functionality of the Second Chance platform. This includes onboarding you as a founder, investor, or partner; managing user accounts and permissions; and enabling the matching, evaluation, and feedback mechanisms that power the platform. For founders, this means processing information such as your pitch deck, business details, and ProofScore inputs to generate automated validation assessments. For investors, this involves handling mandate preferences, stage and sector interests, and custom feedback fields to allow targeted introductions and curated startup updates. Without processing this information, we would be unable to provide the services you expect from Second Chance.

We also use Personal Data to analyze platform performance, understand usage patterns, and improve our technology. This includes collecting and reviewing behavioral and technical data such as page navigation, login frequency, and engagement with evaluation dashboards in order to identify bottlenecks, test new features, and measure the effectiveness of our AI-assisted tools. These insights allow us to make data-informed decisions to enhance the user experience, improve matching accuracy, and refine our validation scoring methodologies. While this data is often anonymized or aggregated for product research purposes, some processing involves identifiable information to support personalized features or troubleshooting.

In addition to operational use, we process contact details and engagement history to maintain communication with our users. We may send you emails or notifications about platform updates, upcoming pitch events, product improvements, or cohort announcements. These communications are designed to keep you informed and connected to relevant opportunities. We will always offer you the ability to opt out of non-essential marketing communications. However, messages directly related to your use of the

platform such as onboarding reminders, matched introductions, or mandatory updates will continue as necessary for the provision of our services.

For investors and strategic partners, we may use profile and preference data to facilitate curated introductions to selected founders. This includes notifying you of new founder cohorts, sharing summary validation outputs, and enabling warm intros where a mutual interest is identified. Such activities are designed to ensure relevance and efficiency in the investor-founder matching process, and are carried out in accordance with our legitimate interests and those of our users.

We also process Personal Data for compliance and legal purposes. This may include responding to lawful requests from regulatory authorities, maintaining audit trails, retaining access logs, and meeting any know-your-client (KYC) or anti-money laundering (AML) obligations relevant to our operations or those of our institutional partners. These actions are taken in accordance with applicable UAE regulations, including the PDPL, and international best practices.

To safeguard the platform and our community, we monitor technical and usage data for signs of unauthorized access, fraudulent activity, or violations of our terms of service. Our systems are designed to detect anomalous behavior such as bot traffic, scraping, or brute-force login attempts. We process this data to protect user accounts, maintain the integrity of our systems, and ensure that our services are used in accordance with their intended purpose.

Finally, the Second Chance platform uses automated processing, including artificial intelligence, to generate insights and scores based on startup data. These outputs such as ProofScores, validation layers, and investor matching recommendations are generated through algorithms that analyze structured founder inputs and historical scoring models. However, such evaluations are advisory in nature and are not intended to constitute final investment decisions. Founders and investors retain full responsibility for interpreting and acting upon AI-generated results, and our use of automated processing is subject to appropriate safeguards and human oversight.

In all cases, the lawful basis for processing your Personal Data will be one of the following: the performance of a contract with you; compliance with legal obligations; our legitimate interests in operating and improving the platform; or your explicit consent, where required.

5: Lawful Basis for Processing

East Emblem Ltd processes Personal Data in accordance with the legal requirements set out in Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL), which is the principal data protection legislation in the United Arab Emirates, as well as applicable international standards where relevant. We ensure that every instance of data processing is based on a clearly defined lawful basis, and that individuals are informed of the rationale behind such processing.

We rely on one or more of the following legal bases when collecting or using Personal Data, depending on the specific context and nature of the interaction:

1. Contractual Necessity

We process Personal Data when it is necessary to enter into or perform a contract with you. This includes enabling you to register for and access the Second Chance platform, participate in evaluations, receive investor introductions, or access advisory tools. Without this data, we would not be able to provide our core services to you.

For example, if you are a founder using the platform to submit your startup for evaluation or to be matched with potential investors, we require your contact details, submission documents, and profile information in order to fulfill that service. Similarly, if you are an investor receiving curated introductions, we must process information related to your mandate and preferences to ensure relevance and quality.

2. Consent

In some situations, we ask for your explicit consent before processing your Personal Data. This typically applies to non-essential marketing communications, the placement of certain cookies or trackers on your device, or the use of optional services such as video features, third-party integrations, or participation in case studies and testimonials.

Where consent is the basis for processing, it will always be presented clearly, separately from other terms, and obtained through an affirmative action (such as checking a box or clicking "I agree"). You may withdraw your consent at any time by contacting us at info@eastemblem.com, and we will act promptly to cease processing for that specific purpose.

3. Legitimate Interests

We also process Personal Data where it is necessary for the purposes of our legitimate interests, provided that such interests are not overridden by your rights, freedoms, or reasonable expectations. Our legitimate interests include: improving the functionality of the platform; conducting analytics and usage research; maintaining security and fraud prevention systems; and promoting the growth of the Second Chance ecosystem through limited, relevant outreach.

This legal basis allows us to support platform innovation, ensure a smooth user experience, and build meaningful founder-investor connections, while taking care to minimize the impact on your privacy. We carefully assess all legitimate interest uses through internal balancing tests and apply safeguards such as pseudonymization, data minimization, and opt-out controls wherever appropriate.

4. Legal Obligations

We may process your Personal Data when it is required to comply with applicable legal or regulatory obligations. This includes obligations under UAE law, including Masdar City Free Zone regulations, tax authority requirements, contractual commitments to our institutional clients, and in some cases requests from courts, regulators, or enforcement authorities.
Such processing may involve storing records for prescribed retention periods, sharing information with lawful authorities, or conducting verification processes for KYC/AML purposes in collaboration with qualified partners.

5. Public Interest or Protection of Vital Interests

In rare cases, we may process Personal Data to protect the vital interests of a person or for reasons of substantial public interest, such as in the event of a security breach, a legal

claim, or a situation involving urgent risk to safety or rights. We will only rely on this ground where there is no less intrusive or alternative way to achieve the intended purpose.

Each processing activity described in this policy is supported by at least one of the lawful bases outlined above. Where multiple bases apply, we rely on the most specific and appropriate basis for each purpose. We are committed to ensuring that your data is handled lawfully, fairly, and transparently at all times, and we will never use your Personal Data for purposes that are incompatible with the original purpose of collection without informing you and, where required, obtaining your consent.

6: Data Sharing and Third Parties

East Emblem Ltd takes the privacy and confidentiality of your Personal Data seriously. We do not sell, license, or trade your Personal Data for commercial gain. However, in order to operate the Second Chance platform effectively, deliver our services, and comply with legal and technical obligations, we may share Personal Data with trusted third parties under clearly defined conditions and safeguards.

We only share Personal Data when it is necessary, proportionate, and lawful to do so. Each recipient is carefully vetted, and appropriate contractual, organizational, and technical measures are implemented to ensure the security and integrity of your information.

6.1 Sharing with Investors and Strategic Partners

One of the core functions of the Second Chance platform is to facilitate curated introductions between founders and potential investors. If you are a founder and choose to participate in the platform, certain Personal Data about you and your startup may be shared with selected investors whose mandates align with your profile. This may include pitch deck content, ProofScores, summary validation outputs, and limited contact information, along with custom notes or comments derived from platform interactions.
These investor recipients are contractually bound by confidentiality restrictions and are only permitted to use this information for internal evaluation and decision-making purposes. Investors are not allowed to share or redistribute founder information outside their organizations without express consent.

Similarly, if you are an investor or partner engaging with the platform, we may share basic information with founders as part of the matching or warm intro process for example, your name, firm, stage/sector interest, and publicly available affiliation details. You have the option to customize your visibility preferences or withdraw from the matching process at any time.

6.2 Sharing with Service Providers and Vendors

We rely on reputable third-party service providers to support the technical and operational delivery of the Second Chance platform. These vendors include cloud hosting providers (e.g. Amazon Web Services), analytics tools (e.g. Google Analytics, Amplitude), customer relationship and marketing platforms, communication tools, and security monitoring services.

These providers act as Data Processors on our behalf. They are contractually obligated through Data Processing Agreements (DPAs) to:

- Process your Personal Data only in accordance with our written instructions;
- Maintain strict confidentiality and data protection standards;
- Implement appropriate technical and organizational security measures;
- Assist us with auditability, data access requests, or breach notification obligations.

We do not authorize these service providers to use or disclose your Personal Data for their own commercial purposes.

6.3 Sharing within the East Emblem Group and Successor Entities
If East Emblem undergoes a corporate transaction such as a merger, acquisition, restructuring, or sale of assets, Personal Data may be transferred to the new or acquiring entity as part of the continuity of business operations. In such cases, we will take all appropriate measures to ensure that the receiving entity is subject to the same or substantially equivalent obligations with respect to data protection and privacy.

We may also share data internally between affiliated entities or controlled subsidiaries of East Emblem for operational purposes, provided that such sharing is compliant with applicable laws and internal access controls.

6.4 Legal Disclosures and Government Requests
We may disclose your Personal Data where required to comply with applicable laws, regulations, court orders, or lawful requests from public authorities or regulatory agencies, including authorities in the UAE. Such disclosures may be made to:

- Respond to subpoenas or legal proceedings;
- Cooperate with government investigations or regulatory inquiries;
- Prevent, detect, or investigate security incidents, fraud, or other unlawful activity;
- Protect the rights, property, or safety of East Emblem, its users, or others.

Where permitted, we will notify you if your Personal Data is subject to such a disclosure.

6.5 Sharing for Audit, Legal, or Professional Advice
We may grant limited access to Personal Data to our external auditors, legal counsel, or advisors where necessary to fulfill regulatory reporting obligations, resolve disputes, enforce our terms, or obtain professional guidance. Such access is strictly controlled and limited to the minimum necessary scope.

East Emblem ensures that all data-sharing arrangements are governed by appropriate legal safeguards, such as data sharing agreements, confidentiality clauses, and (where applicable) Standard Contractual Clauses or equivalent mechanisms for international transfers. We remain accountable for the processing of your Personal Data by any third parties acting on our behalf and regularly review our relationships to ensure ongoing compliance.

7: AI-Generated Insights and Responsibility Disclaimer

The Second Chance platform uses automated systems, including artificial intelligence (AI) and machine learning models, to support the analysis, scoring, and validation of founder submissions. These systems are integral to our ability to process high volumes of startup

information efficiently, generate structured insights for investors, and provide founders with objective, consistent feedback on their readiness, strengths, and gaps.

When you submit materials to the platform such as your pitch deck, founder profile, traction data, or milestone roadmap our systems may apply algorithmic models to assess your startup's stage, progress, and alignment with investor mandates. These models help generate outputs such as ProofScores, validation layers, and investor matching scores, all of which are designed to assist with benchmarking, routing, and decision-making.
It is important to understand that these AI-generated outputs are advisory in nature. They are designed to augment human understanding, not to replace it. All results and scores should be interpreted as inputs into a broader decision-making process. Neither East Emblem nor its algorithms make investment decisions, endorsements, or funding recommendations on behalf of any party.

Founders remain fully responsible for the accuracy of the information they provide and for interpreting the outcomes shared by the platform. Investors remain solely responsible for their own due diligence, risk assessment, and funding decisions. We encourage all users whether founders, investors, or partners to treat AI-generated content as one of several tools available to guide their decision-making.

Where AI systems are used, we apply robust internal governance measures to ensure transparency, accuracy, and fairness. Our algorithms are regularly reviewed for bias, drift, and unintended outcomes. We avoid deploying fully automated systems for any decisions that may have legal or significant effects on individuals, such as platform exclusion, investment qualification, or ranking visibility, without human oversight.

If you believe that an AI-generated evaluation or decision may be inaccurate or unfair, you are encouraged to contact us at info@eastemblem.com to request a review. We are committed to providing meaningful explanations of how automated assessments are conducted, what inputs they rely on, and what steps can be taken to challenge or contextualize a result.

In accordance with the UAE PDPL and international data protection frameworks, you have the right not to be subject to solely automated decisions that significantly affect your legal or personal interests without appropriate safeguards in place. East Emblem complies with these requirements and ensures that meaningful human involvement is maintained wherever required.

8: Marketing, Communications & Preferences

East Emblem Ltd may, from time to time, contact you with information about the Second Chance platform, new features, founder or investor opportunities, partner events, or content that we believe may be relevant or beneficial to you. These communications may include newsletters, updates, invitations to pitch events or investor roundtables, feature announcements, or periodic surveys.

We aim to communicate with you in a thoughtful, relevant, and respectful manner, and to give you meaningful control over how we use your contact details for marketing or outreach purposes.

If you are a founder, we may contact you with:

- Updates about your application or evaluation
- Opportunities for additional support or visibility (e.g., inclusion in an upcoming cohort or showcase)
- Announcements about platform changes or partner initiatives

If you are an investor or partner, we may share:

- Introductions to relevant founders
- Cohort summaries or spotlight profiles
- Invitations to participate in demo days, discovery sessions, or validation pilot groups

We send these communications based on either your explicit consent (e.g., opting in via a form or checkbox) or our legitimate interest in keeping platform participants informed and engaged always in a manner that is non-intrusive and aligned with your role and expectations.

You may opt out of non-essential communications at any time by:

- Clicking the unsubscribe link at the bottom of our emails
- Adjusting your communication preferences via your platform account (where applicable)
- Contacting us directly at info@eastemblem.com

Opting out of marketing communications will not affect transactional or operational messages, such as updates about your account, introductions, security notices, or required compliance correspondence. These service-related messages are essential for the delivery of the platform and cannot be disabled without deactivating your user account.

We will never send you direct marketing without an appropriate legal basis and will not share your contact information with third parties for their own marketing purposes without your express consent. Where required by law, we will request affirmative opt-in consent before sending you promotional content.
If you previously gave consent to receive marketing communications but no longer wish to receive them, you may withdraw that consent at any time using the methods described above. We will act promptly to update your preferences in our systems.

9: Cookies and Tracking Technologies

East Emblem Ltd uses cookies and other tracking technologies to enhance the performance, functionality, and usability of the Second Chance platform. These technologies help us understand how visitors engage with our content, monitor site performance, enable secure logins, personalize features, and improve the overall user experience.

Cookies are small text files stored on your device when you visit or interact with a website or application. They allow us to remember your preferences, recognize returning users, and deliver features in a consistent and secure manner. Some cookies are set by us directly (first-party cookies), while others may be placed by third-party service providers whose tools or analytics are integrated into the platform.

9.1 Types of Cookies We Use

We use the following categories of cookies and similar tracking technologies:

Essential Cookies
These cookies are necessary for the platform to function properly and securely. They enable basic functionality such as user login, session authentication, CSRF protection, and navigation. Because they are required for the site to operate, you cannot opt out of essential cookies through platform settings.

Performance and Analytics Cookies
These cookies collect information about how users interact with the platform, such as which pages are visited, how long users stay on certain sections, which links are clicked, and whether any errors occur. This data helps us understand user behavior, measure engagement, and improve the effectiveness of our layout, content, and features. We may use tools such as Google Analytics or Amplitude to collect and process this data. Where required by law, these cookies will only be activated with your consent.

Functional Cookies
These cookies enable the platform to remember choices you make, such as language preferences, view settings, or form autofill values. They allow us to personalize your experience and reduce friction when returning to the site. Functional cookies may be disabled in your browser, but doing so may impact usability.

Targeting and Third-Party Cookies
In limited cases, we may partner with trusted third-party services to display relevant platform updates or partnership content through advertising or embedded media. These cookies may track user behavior across websites for the purpose of measuring engagement or optimizing reach. We will always seek your consent before enabling these cookies and will provide clear instructions on how to opt out.

9.2 Cookie Consent and Control
When you visit the Second Chance platform for the first time (or after clearing your cookies), you will be presented with a cookie banner or consent manager that allows you to review and manage your cookie preferences. You may choose to accept all cookies, reject non-essential ones, or customize your preferences according to cookie category.
You may also manage cookies through your browser settings. Most browsers allow you to view, delete, or block cookies for specific websites. Please note that disabling cookies may affect certain features and functionality of the platform.

Where required by the UAE PDPL or similar laws, we will not set non-essential cookies without your prior, affirmative consent. We keep detailed records of cookie consent and will refresh consent periodically in accordance with regulatory guidance.

9.3 Web Beacons, Pixels, and Device Fingerprinting
In addition to cookies, we may use other tracking mechanisms such as:

- Web beacons or tracking pixels, which allow us to monitor email opens, link clicks, and session behavior.
- Session tokens, which associate your activity with your logged-in profile without storing personal identifiers in cookies.
- Device fingerprinting methods for security and fraud prevention, which help detect unauthorized or suspicious access patterns.

These technologies serve security, analytics, and feature enablement purposes and are used in a manner consistent with our privacy obligations. Where feasible, we minimize the use of intrusive technologies and seek consent when required.

9.4 Contact and Additional Information

If you have any questions about how we use cookies or tracking technologies or if you wish to withdraw or change your cookie preferences you may contact us at info@eastemblem.com at any time.

A standalone Cookie Policy with updated details about individual cookies and third-party providers may also be available on our website or platform interface.

10: Data Transfers Outside the UAE

As a digital platform with a globally distributed user base and service infrastructure, East Emblem Ltd may, from time to time, transfer Personal Data outside the United Arab Emirates, including to countries that may not offer the same level of data protection as the UAE or the user's country of residence.

These transfers may occur for various operational reasons, such as when we:

- Use third-party cloud infrastructure or hosting providers based abroad (e.g., AWS or other secure cloud platforms);
- Engage data processors or service providers (such as analytics tools or communication platforms) located in foreign jurisdictions;
- Interact with investors, partners, or founders based outside the UAE in the context of Second Chance introductions or platform services.

Where such international transfers are necessary, we take appropriate legal and technical measures to ensure that your Personal Data remains protected, secure, and handled in a manner that is consistent with the rights and obligations set out in the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL), as well as relevant international frameworks such as the EU GDPR, where applicable.

10.1 Transfer Safeguards

In accordance with Article 23 of the UAE PDPL, we only transfer Personal Data outside the UAE if one of the following conditions is met:

- The recipient jurisdiction has been deemed to offer an adequate level of protection by the UAE Data Office or other recognized authority;
- We have entered into legally binding instruments, such as Standard Contractual Clauses (SCCs) or equivalent data transfer agreements, with the receiving party to ensure the data is processed in accordance with UAE and international data protection standards;

- The transfer is otherwise justified by explicit consent from the Data Subject, contractual necessity, legal obligation, or to protect the vital interests of the individual.

Where appropriate, we also implement additional technical safeguards, such as encryption, pseudonymization, role-based access control, and storage limitation to reduce the risk of unauthorized access or misuse during or after transfer.

10.2 Transfers to Multinational or Cross-Border Teams
Some members of the East Emblem team including analysts, product managers, and data scientists may be located outside the UAE. Where such personnel access Personal Data in the course of delivering platform services, they do so under strict internal policies and access controls. All East Emblem employees and contractors are subject to confidentiality obligations and privacy training regardless of their location.

Where access is granted from jurisdictions without an adequacy ruling, we ensure that it is limited to only what is necessary, secured through encrypted connections, and subject to oversight by our UAE-based data governance function.

10.3 Your Rights in International Transfers
You have the right to be informed when your Personal Data is transferred to another country, and to request further information about the safeguards we have put in place. If you would like more detail about our cross-border data transfer arrangements, including the list of service providers and data processors located abroad, you may contact us at info@eastemblem.com.

We will provide you with a response in accordance with our legal obligations and with respect for the commercial sensitivity of our security architecture.

11: Data Security Measures

East Emblem Ltd is committed to protecting the confidentiality, integrity, and availability of the Personal Data we collect and process through the Second Chance platform. We implement a robust framework of technical, organizational, and contractual security measures to safeguard data against unauthorized access, accidental loss, destruction, misuse, or unlawful disclosure.

Our data security program is built on internationally recognized standards and is regularly reviewed to ensure that it evolves in response to emerging threats, legal developments, and platform changes.

11.1 Technical Safeguards
All Personal Data processed by East Emblem is hosted on secure cloud infrastructure using trusted service providers that comply with high-grade security certifications (e.g., ISO 27001, SOC 2). Our infrastructure is designed to ensure fault tolerance, redundancy, and data encryption both at rest and in transit.

We use HTTPS/SSL encryption for all communications between user devices and our servers, enforce strong access credentials, and apply multi-factor authentication (MFA) for administrative or privileged user accounts. Role-based access controls (RBAC) are in place

to ensure that only authorized personnel may access specific categories of data relevant to their function.

Audit logs are maintained to record system access, data changes, and permission modifications, enabling traceability and post-incident forensics if required. Passwords are securely hashed using modern cryptographic standards and are never stored in plain text.

11.2 Organizational Safeguards
All East Emblem employees, consultants, and contractors with access to Personal Data are subject to strict confidentiality obligations and undergo regular privacy and security training. Personnel are trained to recognize and respond to phishing, social engineering attempts, and data handling risks.

We maintain an internal data classification framework to distinguish between public, internal, sensitive, and restricted information. Data minimization practices are applied to limit collection and retention to what is necessary for each specific use case.

All devices used by East Emblem staff must comply with security policies that include endpoint encryption, automatic locking, screen timeout, and mandatory software updates. Remote access is secured through VPN and endpoint protection tools.

Where third-party processors or service providers handle data on our behalf, we ensure they are contractually bound to uphold equivalent security standards through detailed Data Processing Agreements (DPAs). These contracts also include audit rights, breach notification clauses, and access restrictions.

11.3 Physical and Environmental Security
Although East Emblem operates primarily through cloud-based systems, any physical locations or on-premises storage (e.g., for partner events or workshops) are subject to physical access controls, locked storage, and secure disposal protocols. Any hard-copy records are stored in locked cabinets and disposed of via shredding or certified destruction services when no longer needed.

11.4 Vulnerability Management and Monitoring
Our systems are continuously monitored for suspicious behavior, unauthorized access attempts, and performance anomalies. We perform routine vulnerability scans, dependency reviews, and (where appropriate) third-party penetration tests to identify and address weaknesses.

Software updates and patches are applied regularly to protect against known threats, and change management policies govern updates to platform components and infrastructure configurations.

11.5 Business Continuity and Disaster Recovery
East Emblem maintains backup and recovery procedures to ensure the continuity of service in the event of data loss, system failure, or disaster scenarios. Backups are encrypted and stored in geographically redundant locations. Business continuity plans are reviewed and tested periodically to verify readiness and alignment with operational risk thresholds.

We take seriously our responsibility to keep your data safe and secure, and we continuously invest in improvements to our technical systems, employee awareness, and platform resilience. However, it is important to recognize that no system can guarantee absolute security. If you suspect any misuse or unauthorized access to your data, please contact info@eastemblem.com immediately so we can investigate and take appropriate action.

12: Data Retention

East Emblem Ltd retains Personal Data only for as long as it is necessary to fulfill the specific purposes for which it was collected, or to comply with applicable legal, regulatory, or contractual requirements. Once the relevant purpose has been satisfied or the applicable retention period has expired we will securely delete, anonymize, or archive the data in accordance with our internal retention and disposal policies.

Our data retention framework is designed to support the following goals:

- Ensure data is kept no longer than necessary;
- Comply with relevant UAE data protection laws, including Article 10 of the UAE PDPL;
- Maintain the ability to respond to audits, regulatory inquiries, or legal claims;
- Mitigate the risk of unauthorized access by minimizing data sprawl or duplication.

12.1 Retention Periods by Use Case

Personal Data is retained for different durations depending on the nature of the relationship and the purpose for which it was collected. For example:

- Founders and startup applicants: Data submitted to the Second Chance platform (e.g. pitch decks, ProofScores, onboarding forms) is retained for the duration of your engagement with the platform and up to 24 months following your last login or activity, unless earlier deletion is requested. This allows us to maintain historical scoring data, performance benchmarking, and access for potential investors during follow-on periods.
- Investors and partners: Investor profiles, preferences, and engagement history are retained for the duration of your relationship with East Emblem and for up to 36 months after your last interaction, to support ongoing curation and cohort access. You may request that we anonymize your account at any time while preserving your firm’s interaction history for analytics purposes.
- Email communications, support logs, and feedback surveys: These records are typically retained for up to 18 months, unless a longer period is required for legal or audit purposes.
- Security logs, authentication data, and system access records: Retained for 12 to 24 months, depending on risk classification and jurisdictional obligations.
- Financial and invoicing records: Retained for a minimum of 5 years, as required by UAE commercial regulations and accounting standards.

Where we are legally required to retain records beyond the periods noted above for example, due to court orders, tax laws, or regulatory audits we will comply accordingly.

12.2 Anonymization and Aggregation

In some cases, we may retain data in an anonymized or aggregated form after the original retention period has expired. This means the data is no longer associated with an

identifiable individual and cannot be used to re-identify a person. Aggregated data may be used for analytics, benchmarking, or research purposes and does not fall within the scope of Personal Data under this policy.

12.3 Secure Disposal and Deletion
At the end of a retention period, or upon valid request for erasure, we take reasonable steps to securely delete or de-identify Personal Data from our systems. This includes:

- Overwriting or cryptographic wiping of digital records;
- Physical destruction of paper records, where applicable;
- Ensuring that backups containing Personal Data are either deleted on rotation or flagged for erasure at the next recovery cycle.

Deletion processes are applied across production, test, and backup environments to ensure consistency. We maintain audit records of deletion activities in accordance with our internal compliance policies.

12.4 Data Subject-Initiated Deletion
You may request deletion of your Personal Data at any time, subject to any legal or operational obligations that require us to retain it. If no such obligations apply, we will honor your request and confirm deletion within a reasonable timeframe. See Section 14: Data Subject Rights for more information on your right to erasure.

We periodically review all categories of Personal Data held by East Emblem to ensure ongoing alignment with our retention policy and to minimize unnecessary data storage. If you have questions about how long your data is retained, or would like to initiate a deletion request, please contact us at info@eastemblem.com.

13: Data Subject Rights
East Emblem Ltd respects your rights as a data subject and is committed to ensuring that you can exercise meaningful control over your Personal Data in accordance with the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) and, where applicable, global privacy regulations such as the EU General Data Protection Regulation (GDPR).

If you interact with the Second Chance platform as a founder, investor, partner, or visitor you have a range of rights regarding your Personal Data. We take these rights seriously and have procedures in place to address any request you may make in a timely, transparent, and secure manner.

13.1 Your Rights
As a data subject, you may exercise the following rights:

1. Right to Access
   You have the right to request confirmation of whether we hold Personal Data about you and, if so, to access that information. Upon request, we will provide a copy of the data we process, along with details about its source, purpose, categories, and any third parties with whom it has been shared.

2. Right to Rectification

If you believe that any Personal Data we hold about you is inaccurate, incomplete, or outdated, you have the right to request that it be corrected or updated. We will take reasonable steps to verify and make the necessary amendments.

3. Right to Erasure (Right to be Forgotten)
   You have the right to request deletion of your Personal Data under certain conditions such as when it is no longer needed for the purpose it was collected, when consent is withdrawn, or when processing is unlawful. We will evaluate each request in light of any legal or contractual obligations requiring data retention and inform you of the outcome.

4. Right to Object to Processing
   You may object to the processing of your Personal Data where the processing is based on our legitimate interests or relates to direct marketing. If your objection is valid, we will cease processing the data unless we can demonstrate compelling legal grounds to continue.

5. Right to Restrict Processing
   In certain situations, you may request that we temporarily suspend processing of your data such as while verifying its accuracy or reviewing an objection request. During this period, we will not use the data for any purpose other than storage..

6. Right to Data Portability
   Where processing is based on consent or contract, and is carried out by automated means, you may request to receive your Personal Data in a structured, commonly used, machine-readable format, and to have it transmitted to another controller, where technically feasible.

7. Right to Withdraw Consent
   Where we rely on your consent to process Personal Data such as for marketing communications you may withdraw your consent at any time. Withdrawal does not affect any processing that took place prior to your request.

8. Right to Lodge a Complaint
   If you believe your rights have been violated or that we have not handled your Personal Data in accordance with the law, you have the right to lodge a complaint with the UAE Data Office, or with the relevant supervisory authority in your country of residence, if applicable.

13.2 How to Exercise Your Rights
To exercise any of the rights outlined above, you may contact us at:
Email: info@eastemblem.com

Subject line: "Data Request – [Your Name or Organization]"

We may ask you to verify your identity before fulfilling your request, particularly if the request concerns sensitive data or could impact another party's rights. We aim to respond to all valid requests within 30 days, although complex requests may take longer. In such cases, we will keep you informed of progress.

Please note that your rights may be subject to certain legal exceptions or limitations. For example, we may decline a request if fulfilling it would infringe on the rights of another individual, violate a legal obligation, or compromise a legitimate investigation.

At East Emblem, we believe that data protection is not only a legal obligation, but also a foundation of trust. If you have any questions or concerns about your rights or how to exercise them, we encourage you to reach out directly to our privacy team.

14: Data Breach Notification and Incident Response

East Emblem Ltd maintains a proactive and structured incident response protocol designed to detect, contain, assess, and mitigate any actual or suspected breach of Personal Data. While we implement robust security safeguards to minimize the risk of incidents, we also recognize the importance of being prepared to act decisively if a breach occurs.

In accordance with Article 9 of the UAE Personal Data Protection Law (PDPL) and applicable international frameworks, East Emblem commits to timely and transparent notification procedures in the event of any breach that poses a risk to the confidentiality, integrity, or availability of Personal Data.

14.1 What Constitutes a Data Breach?
A data breach may include, but is not limited to:

- Unauthorized access to Personal Data by a third party (e.g., hacking or phishing attack);
- Accidental disclosure or loss of data due to human error or system malfunction;
- Malicious data corruption or ransomware attacks;
- Internal misuse of Personal Data in violation of access policies.

Breaches may involve data in digital or physical form and can result from acts of omission, negligence, or deliberate wrongdoing.

14.2 Our Response Process
If we detect or are informed of a potential data breach, we immediately activate our incident response plan, which includes the following steps:

1. Detection & Containment
   We isolate affected systems to prevent further exposure or escalation and begin assessing the scope of the breach.

2. Assessment & Classification
   We evaluate the type of data involved, the number of individuals affected, the root cause, and the potential consequences for users or stakeholders.

3. Notification of Authorities
   If the breach presents a risk to the privacy, security, or rights of individuals, we notify the UAE Data Office (or other competent authority) within the legally

mandated timeframe. This includes details of the incident, potential impact, mitigation measures, and steps taken to prevent recurrence.

4. Notification of Affected Individuals
   Where required by law or where we believe it is necessary to protect your interests we will notify affected individuals promptly. Notifications will describe the nature of the breach, any data affected, recommended steps you can take to reduce potential harm (e.g., password resets), and how to contact us for further information.

5. Remediation & Prevention
   We take corrective actions to fix the root cause of the incident, including security patches, access changes, policy revisions, and employee re-training. A post-incident review is conducted to document lessons learned and enhance our protocols.

14.3 Your Role in Security
While we maintain strong technical and organizational security controls, the protection of your Personal Data also depends on your cooperation. You are responsible for safeguarding your login credentials, not sharing access with unauthorized parties, and promptly reporting any suspicious activity involving your account.

If you suspect that your data may have been compromised whether through phishing, unauthorized account access, or platform misuse you should immediately contact us at info@eastemblem.com.

East Emblem is committed to accountability, transparency, and rapid response in the event of a breach. We treat all incidents with the urgency and seriousness they deserve, and we view breach response not as a compliance obligation but as a critical part of maintaining trust with our community.

15: Contact Information and Policy Updates

East Emblem Ltd is committed to maintaining transparency, accountability, and responsiveness in all matters concerning your Personal Data. If you have any questions, concerns, or requests relating to this Privacy Policy or to how your data is collected, processed, or protected you are encouraged to contact us using the details below.

15.1 Contacting East Emblem

If you wish to:
- Make a data subject request (e.g., access, deletion, rectification);
- Report a suspected data breach or security concern;
- Withdraw consent or update your communication preferences;
- Lodge a complaint or seek clarification about our data practices;

You may contact our privacy and compliance team at:
Email: info@eastemblem.com

Subject line: “Privacy Inquiry – [Your Name or Company]”

We will acknowledge and respond to your request in accordance with applicable legal timeframes. If your concern cannot be resolved internally, you have the right to escalate it to the UAE Data Office or another relevant supervisory authority, depending on your jurisdiction.

15.2 Policy Updates

We may update this Privacy Policy from time to time to reflect changes in:

- Applicable data protection laws or regulatory requirements;
- Our internal practices, platform features, or service offerings;
- Technology or security infrastructure improvements.

All updates will be posted to our website or platform with a revised "Last Updated" date. In the case of material changes particularly those affecting your rights or how we use your Personal Data we will provide additional notice (e.g., by email or on-platform banners) and, where required, request renewed consent.

We encourage all users to review this Privacy Policy periodically to stay informed of how we protect your information.