



KEYSECURE PRIVACY POLICY

Last Updated: 26 June 2026

This Privacy Policy (“Privacy Policy”) describes how KeySecure Hong Kong Limited (“KeySecure”, the “Company”, “we”, “our”, or “us”) collects, receives, records, uses, processes, stores, transfers, discloses, shares, retains, analyzes, safeguards, and otherwise handles Personal Data in connection with your access to and use of the KeySecure website, mobile applications, virtual payment card services, cryptocurrency payment services, Crypto Asset conversion services, APIs, software, technologies, and any related products, features, or services made available by KeySecure from time to time (collectively, the “Services”).

By accessing, downloading, registering for, interacting with, or otherwise using the Services, you acknowledge, represent, warrant, and agree that you have carefully read, fully understood, and accepted this Privacy Policy and that KeySecure may collect, use, process, transfer, disclose, retain, analyze, and otherwise handle your Personal Data in accordance with this Privacy Policy, the Terms & Conditions, and Applicable Laws.

1. Data Controller

- 1.1.** For the purposes of Applicable Laws relating to data protection and privacy, KeySecure shall act as the data controller in relation to the collection, use, processing, disclosure, transfer, retention, and other handling of Personal Data described in this Privacy Policy unless otherwise expressly stated. The relevant KeySecure entity acting as data controller may vary depending on the jurisdiction, Services used, operational structure, regulatory requirements, or relationship with the User.
- 1.2.** Users may contact KeySecure regarding privacy, data protection, or Personal Data processing matters using the contact details set out in this Privacy Policy.

2. Definitions

For the purposes of this Privacy Policy, the following terms shall have the meanings set forth below:

“Applicable Laws” means all applicable laws, statutes, ordinances, regulations, rules, directives, notices, circulars, codes, regulatory requirements, supervisory expectations, governmental guidance, judicial decisions, decrees, judgments, orders, sanctions regimes, industry standards, legally binding obligations, and requirements imposed, issued, administered, enforced, or interpreted by any governmental authority, regulator, supervisory authority, court, tribunal, arbitral body, enforcement agency, self-regulatory organization, stock exchange, payment network, sanctions authority, tax authority, or other competent authority in any relevant jurisdiction.

“Crypto Assets” means cryptocurrencies, stablecoins, virtual assets, and other blockchain-based digital representations of value that are supported, facilitated, processed, converted, transferred,



stored, settled, or otherwise made available through the Services by KeySecure from time to time.

“Personal Data” means any information, data, record, identifier, or combination of information relating to, describing, identifying, capable of identifying, or reasonably capable of being associated, directly or indirectly, with an identified or identifiable natural person, household, device, account, or user, including any information defined as personal data, personal information, personally identifiable information, consumer information, or similar terminology under Applicable Laws.

“Platform” means the KeySecure websites, mobile applications, APIs, software systems, databases, interfaces, payment systems, technologies, infrastructure, communication systems, wallet systems, operational environments, and all related digital or technological systems, networks, functionalities, and infrastructure through which the Services are made available, operated, facilitated, administered, or supported.

“Services” means the card issuance, card account management, crypto-to-fiat conversion, payment processing, settlement services, transaction monitoring, account administration, customer support, APIs, platform functionalities, and any related products, features, technologies, tools, or services made available by KeySecure from time to time.

3. Collection of Personal Data

- 3.1.** KeySecure may, to the fullest extent permitted by Applicable Laws, collect, receive, obtain, access, record, organize, structure, store, retain, adapt, modify, retrieve, consult, use, process, analyze, monitor, combine, correlate, derive, disclose, transfer, share, transmit, disseminate, archive, or otherwise handle Personal Data obtained directly or indirectly from Users, automatically through the access to or use of the Services, from affiliated entities, group companies, banking partners, custodians, payment processors, blockchain networks, Crypto Asset protocols, third-party service providers, compliance vendors, analytics providers, fraud prevention providers, sanctions screening providers, publicly available sources, governmental authorities, law enforcement agencies, or any other lawful third-party sources, for any purposes deemed necessary, appropriate, advisable, or desirable by KeySecure in connection with the provision, operation, administration, maintenance, security, improvement, compliance, monitoring, risk management, enforcement, analytics, or protection of the Services and the legitimate business interests of KeySecure and its affiliates.

4. Information Provided by Users

- 4.1.** KeySecure may collect, receive, record, verify, process, analyze, store, retain, and otherwise handle Personal Data voluntarily provided, submitted, transmitted, uploaded, disclosed, or otherwise made available by Users in connection with the access to or use of the Services, including but not limited to full legal names, residential addresses, correspondence addresses, email addresses, telephone numbers, nationality and citizenship information, dates of birth, government-issued identification documents, passport information, national identification numbers, photographs, selfie images, biometric verification information, facial recognition data, liveness detection information, tax identification information, employment information, wallet



addresses, blockchain identifiers, bank account details, payment information, source-of-funds information, source-of-wealth information, transaction explanations, declarations, certifications, attestations, supporting documentation, and any other information, records, or materials requested or obtained for compliance, verification, onboarding, operational, security, legal, regulatory, fraud prevention, risk management, investigative, or other lawful business purposes deemed necessary or appropriate by KeySecure in its sole discretion.

5. Information Collected Automatically

- 5.1.** When Users access, browse, interact with, or otherwise use the Services, KeySecure may automatically collect, generate, receive, monitor, record, analyze, derive, correlate, process, and retain technical, operational, behavioral, device-related, and usage-related information, including but not limited to Internet Protocol (IP) addresses, device identifiers, device metadata, device fingerprinting information, browser types, operating systems, hardware identifiers, application version information, authentication records, login records, access timestamps, session identifiers, cookies, web beacons, software development kits (SDKs), advertising identifiers, behavioral analytics, browsing activities, usage patterns, clickstream data, telemetry data, network identifiers, approximate geolocation data, risk indicators, connectivity information, technical logs, operational records, and other technical or usage-related information associated with the access to or use of the Services.
- 5.2.** To the extent permitted by Applicable Laws, KeySecure may use, process, analyze, combine, correlate, and otherwise handle such information for purposes including but not limited to fraud prevention, cybersecurity protection, authentication, sanctions screening, transaction monitoring, compliance reviews, anti-money laundering and counter-terrorist financing controls, risk scoring, operational intelligence, analytics, service optimization, machine learning, artificial intelligence model development, behavioral analysis, system administration, security monitoring, incident detection, dispute resolution, regulatory compliance, investigations, enforcement activities, and other lawful operational, commercial, security, compliance, or business purposes deemed necessary or appropriate by KeySecure.

6. Transaction and Blockchain Information

- 6.1.** KeySecure may collect, process, monitor, analyze, store, retain, correlate, disclose, transfer, and otherwise handle records and information relating to blockchain transactions, Crypto Asset transfers, wallet activities, Virtual Card transactions, merchant payment information, fiat settlements, Crypto Asset conversions, transaction hashes (TXIDs), blockchain metadata, transaction timestamps, settlement records, exchange records, smart contract interactions, protocol activities, and related transaction or blockchain information arising out of or relating to the use of the Services.
- 6.2.** Users expressly acknowledge and agree that blockchain networks, Crypto Asset protocols, decentralized systems, and distributed ledger technologies are generally public, decentralized, immutable, transparent, independently operated, and beyond the control of KeySecure, and accordingly blockchain transactions, wallet addresses, transaction hashes, smart contract interactions, and related blockchain information may be permanently recorded, publicly visible,



searchable, traceable, monitored, analyzed, disclosed, and incapable of deletion, reversal, or modification. Users further acknowledge and agree that blockchain transactions and Crypto Asset activities may not be confidential, anonymous, or private, and that information relating to blockchain activities may be visible or accessible to blockchain analytics providers, validators, node operators, governmental authorities, regulators, law enforcement agencies, counterparties, sanctions screening providers, compliance vendors, and other participants or observers on relevant blockchain networks.

- 6.3.** KeySecure does not own, control, operate, supervise, or administer blockchain networks or decentralized systems and shall not be responsible or liable whatsoever for the actions, disclosures, processing activities, accessibility, transparency, storage, retention, publication, monitoring, analysis, or use of information by blockchain networks, validators, node operators, protocol participants, blockchain analytics providers, or any other third parties operating or interacting with decentralized systems or blockchain infrastructure.

7. Information Obtained from Third Parties

- 7.1.** KeySecure may obtain, collect, receive, access, verify, analyze, and otherwise process Personal Data, blockchain intelligence, compliance information, fraud intelligence, risk-related information, and other relevant data from affiliated entities, subsidiaries, banking partners, financial institutions, card issuers, payment processors, custodians, exchanges, liquidity providers, telecommunications providers, blockchain analytics providers, fraud prevention vendors, sanctions screening providers, identity verification providers, cybersecurity vendors, analytics providers, marketing partners, public databases, governmental authorities, regulators, law enforcement agencies, publicly available sources, and other lawful third-party sources.
- 7.2.** Such information may include, without limitation, sanctions information, wallet risk scores, fraud intelligence, blockchain intelligence, transaction monitoring results, adverse media information, device intelligence, compliance records, cybersecurity alerts, enforcement information, risk assessments, behavioral indicators, geolocation data, public blockchain records, and other operational, legal, regulatory, investigative, or risk-related information deemed necessary or appropriate by KeySecure for compliance, fraud prevention, cybersecurity, operational, business, legal, regulatory, enforcement, investigative, or risk management purposes.

8. Purposes of Processing Personal Data

- 8.1.** KeySecure may collect, receive, access, record, organize, structure, store, retain, adapt, retrieve, consult, use, process, analyze, monitor, combine, correlate, derive, disclose, transfer, share, transmit, disseminate, archive, and otherwise handle Personal Data for any lawful, regulatory, operational, commercial, security, compliance, investigative, enforcement, or business purpose relating to or arising from the provision, operation, administration, maintenance, monitoring, security, optimization, protection, improvement, enforcement, or lawful use of the Services, compliance with Applicable Laws, prevention and detection of fraud and financial crime, cybersecurity protection, operational management, dispute resolution, legal proceedings, business administration, and the legitimate business interests of KeySecure, its affiliates, banking partners, custodians, payment processors, card issuers, service providers, and related third parties.



9. Provision and Administration of Services

- 9.1.** KeySecure may collect, use, process, disclose, transfer, retain, and otherwise handle Personal Data for purposes relating to the establishment, verification, administration, maintenance, operation, provision, facilitation, management, support, optimization, and enforcement of the Services, including but not limited to establishing and maintaining user accounts, conducting onboarding and identity verification procedures, administering account access and authentication mechanisms, facilitating Crypto Asset funding and crypto-to-fiat conversion services in connection with card transactions, issuing and administering Virtual Cards, processing payments, settlements, transfers, conversions, and transactions, facilitating merchant payments and settlement activities, managing user preferences and account settings, providing customer support and technical assistance, handling operational inquiries and service requests, conducting operational management activities, and otherwise enabling, operating, supporting, administering, or improving the Services and related functionalities.

10. Compliance, Risk Management, and Security

- 10.1.** KeySecure may collect, use, process, monitor, analyze, disclose, retain, transfer, and otherwise handle Personal Data for purposes relating to compliance, legal obligations, fraud prevention, financial crime prevention, operational security, investigations, enforcement activities, and risk management, including but not limited to conducting know-your-customer ("KYC") procedures, customer due diligence, enhanced due diligence, anti-money laundering ("AML") and counter-terrorist financing ("CFT") compliance activities, sanctions screening, politically exposed person screening, transaction monitoring, blockchain analytics, forensic tracing, fraud prevention, cybersecurity monitoring, operational security assessments, suspicious activity monitoring, investigations, internal audits, dispute resolution, enforcement activities, legal proceedings, regulatory reporting, law enforcement cooperation, compliance reviews, risk scoring, account restrictions, and other compliance, regulatory, operational, security, investigative, enforcement, or risk management activities deemed necessary or appropriate by KeySecure.

11. Analytics, Product Development, and Business Operations

- 11.1.** To the extent permitted by Applicable Laws, KeySecure may collect, use, process, analyze, combine, correlate, derive, retain, and otherwise handle Personal Data and related information for purposes relating to analytics, operational intelligence, machine learning, artificial intelligence model training, behavioral analysis, business intelligence, service optimization, product development, strategic planning, benchmarking, operational performance analysis, fraud detection enhancement, cybersecurity enhancement, market research, internal reporting, quality assurance, business administration, operational management, and other lawful commercial, analytical, research, technological, operational, or business purposes.
- 11.2.** KeySecure may further collect, generate, create, derive, analyze, disclose, transfer, retain, and otherwise use anonymized, aggregated, statistical, de-identified, pseudonymized, or non-personally identifiable information derived from the Services, transactions, blockchain activities, usage patterns, operational data, or related information for any lawful operational, compliance, commercial, analytical, research, benchmarking, machine learning, artificial intelligence, product



development, security, fraud prevention, or business purpose deemed necessary or appropriate by KeySecure.

12. Communications and Marketing

12.1. Subject to Applicable Laws, KeySecure may send, deliver, transmit, publish, or otherwise provide operational notices, security alerts, authentication messages, transaction confirmations, account notifications, compliance notices, service announcements, policy updates, surveys, newsletters, promotional materials, product announcements, marketing communications, and other information relating to the Services, Platform, Crypto Assets, Virtual Cards, products, technologies, features, functionalities, campaigns, events, or business activities of KeySecure or its affiliates through electronic means including email, push notifications, SMS messages, in-app notifications, website postings, APIs, or other communication channels determined by KeySecure.

12.2. Where required under Applicable Laws, Users may opt out of receiving certain marketing communications, provided that KeySecure may continue to send operational, security, compliance, legal, transactional, or account-related communications necessary for the provision, administration, security, or lawful operation of the Services.

13. Legal Basis for Processing

13.1. Where required or applicable under Applicable Laws, KeySecure may collect, use, process, disclose, transfer, retain, and otherwise handle Personal Data based upon one or more lawful bases, including:

- a. performance of contractual obligations and provision of the Services;
- b. compliance with legal, regulatory, compliance, anti-money laundering, sanctions, fraud prevention, tax reporting, cybersecurity, and law enforcement obligations;
- c. legitimate business interests pursued by KeySecure, its affiliates, banking partners, custodians, payment processors, card issuers, service providers, and related third parties, including fraud prevention, cybersecurity, operational administration, analytics, service improvement, investigations, enforcement activities, dispute resolution, business operations, and risk management activities;
- d. protection of vital interests;
- e. public interest considerations;
- f. establishment, exercise, or defense of legal claims;
- g. User consent, where consent is required under Applicable Laws; and
- h. any other lawful basis permitted under Applicable Laws.

13.2. Where KeySecure processes Personal Data based upon legitimate interests, KeySecure may conduct balancing assessments to evaluate whether such legitimate interests are overridden by the rights, freedoms, or interests of Users under Applicable Laws.

13.3. Where required under Applicable Laws, Users may have the right to withdraw consent to certain processing activities at any time, provided that such withdrawal shall not affect the lawfulness of processing conducted prior to such withdrawal and may affect the availability or functionality of certain Services.



14. Disclosure and Sharing of Personal Data

14.1. KeySecure may, to the fullest extent permitted by Applicable Laws, disclose, share, transfer, transmit, provide access to, make available, disseminate, release, exchange, or otherwise provide Personal Data and related information to third parties where KeySecure determines, in its sole and absolute discretion, that such disclosure, sharing, transfer, access, or availability is necessary, appropriate, advisable, desirable, or reasonably required for the provision, operation, administration, maintenance, security, compliance, enforcement, protection, optimization, or lawful use of the Services, compliance with Applicable Laws, protection of the rights and legitimate interests of KeySecure and its affiliates, fraud prevention, cybersecurity, operational management, investigations, dispute resolution, regulatory cooperation, risk management, business administration, or other lawful operational, regulatory, legal, commercial, security, or business purposes.

15. Affiliates and Group Companies

15.1. KeySecure may disclose, transfer, share, provide access to, or otherwise make available Personal Data to its affiliates, subsidiaries, parent companies, related entities, corporate group members, successor entities, and associated companies for purposes including but not limited to operational administration, account management, compliance activities, legal and regulatory obligations, cybersecurity protection, fraud prevention, risk management, analytics, business intelligence, internal reporting, customer support, service optimization, operational efficiency, investigations, enforcement activities, strategic planning, product development, business administration, and other lawful commercial, operational, security, compliance, or business purposes deemed necessary or appropriate by KeySecure.

16. Service Providers and Subprocessors

16.1. KeySecure may engage, appoint, authorize, utilize, or otherwise cooperate with subprocessors, contractors, vendors, infrastructure providers, cloud service providers, cybersecurity providers, identity verification providers, KYC providers, analytics vendors, compliance vendors, blockchain analytics providers, fraud prevention providers, telecommunications providers, customer support providers, banking partners, custodians, exchanges, liquidity providers, payment processors, card issuers, settlement providers, and other third-party service providers to process, store, transmit, analyze, monitor, secure, or otherwise handle Personal Data on behalf of KeySecure for purposes relating to the provision, facilitation, administration, operation, maintenance, compliance, security, optimization, or support of the Services and related business operations.

16.2. KeySecure may provide such third parties with access to Personal Data to the extent deemed necessary, appropriate, or desirable by KeySecure for the performance of their services, functions, obligations, or operational activities.

17. Card Networks and Financial Institutions

17.1. Users expressly acknowledge and agree that Personal Data, transaction information, account information, payment information, Crypto Asset information, and related operational or compliance information may be disclosed, transferred, shared, or otherwise made available to card issuers, card networks, acquiring institutions, settlement providers, banking partners,



financial institutions, payment processors, custodians, merchants, and related financial or payment ecosystem participants for purposes including but not limited to transaction processing, settlement, authorization, fraud prevention, chargeback handling, dispute resolution, sanctions screening, compliance reviews, operational administration, security monitoring, transaction verification, regulatory compliance, financial crime prevention, investigations, enforcement activities, and other lawful operational, compliance, security, or business purposes relating to the provision and operation of the Services.

18. Regulators and Authorities

- 18.1.** KeySecure may disclose, transfer, provide access to, preserve, produce, or otherwise make available Personal Data and related information to courts, regulators, governmental authorities, supervisory bodies, tax authorities, sanctions authorities, law enforcement agencies, enforcement bodies, self-regulatory organizations, arbitral tribunals, competent authorities, financial intelligence units, or other governmental or regulatory entities where such disclosure is required, permitted, requested, compelled, or deemed necessary, appropriate, advisable, or desirable by KeySecure under Applicable Laws or for purposes relating to compliance, fraud prevention, investigations, enforcement activities, regulatory cooperation, dispute resolution, public interest considerations, sanctions compliance, anti-money laundering obligations, counter-terrorist financing obligations, cybersecurity matters, legal proceedings, or the protection of the rights, assets, operations, personnel, or legitimate interests of KeySecure or third parties.
- 18.2.** Users further acknowledge and agree that KeySecure may engage in proactive cooperation, voluntary reporting, suspicious activity reporting, regulatory disclosures, investigative cooperation, information sharing arrangements, and other lawful cooperation activities with competent authorities where deemed necessary or appropriate by KeySecure.

19. Corporate Transactions

- 19.1.** Personal Data and related information may be disclosed, transferred, assigned, novated, shared, provided, or otherwise made available in connection with any actual, proposed, anticipated, or potential merger, acquisition, restructuring, reorganization, financing transaction, joint venture, insolvency proceeding, bankruptcy proceeding, business transfer, corporate reorganization, sale of shares, sale of assets, debt financing, investment transaction, outsourcing arrangement, or other corporate transaction, strategic transaction, or business arrangement involving KeySecure, its affiliates, assets, operations, or business activities.

20. International Transfers of Personal Data

- 20.1.** Users expressly acknowledge, understand, and agree that Personal Data and related information may be transferred, processed, stored, replicated, routed, transmitted, disclosed, retained, monitored, analyzed, or accessed across multiple jurisdictions worldwide where KeySecure, its affiliates, subsidiaries, banking partners, custodians, exchanges, liquidity providers, payment processors, card issuers, cloud providers, infrastructure providers, telecommunications providers, compliance vendors, analytics providers, cybersecurity providers, subcontractors, service providers, or related third parties operate, maintain facilities, conduct business activities, provide services, or otherwise process information in connection with the Services.



20.2. Users further acknowledge and agree that such jurisdictions may have data protection laws, privacy protections, regulatory frameworks, enforcement mechanisms, or legal standards that differ from, and may not provide equivalent levels of protection as, those applicable in the User's jurisdiction of residence or nationality.

20.3. To the extent required under Applicable Laws, KeySecure may implement commercially reasonable safeguards, contractual measures, operational controls, technical protections, organizational safeguards, or other measures deemed appropriate by KeySecure to facilitate and protect international transfers of Personal Data in accordance with Applicable Laws.

21. Data Retention

21.1. KeySecure may retain, preserve, archive, store, process, monitor, analyze, disclose, and otherwise handle Personal Data, blockchain records, communications, compliance documentation, onboarding materials, investigation materials, transaction records, authentication logs, access records, device information, analytics data, forensic reports, operational records, cybersecurity logs, wallet information, blockchain intelligence, and related information for such periods as KeySecure determines, in its sole and absolute discretion, to be necessary, appropriate, prudent, advisable, or desirable for purposes including but not limited to compliance with Applicable Laws, anti-money laundering and know-your-customer obligations, fraud prevention, cybersecurity protection, investigations, dispute resolution, enforcement activities, legal proceedings, regulatory cooperation, operational administration, business continuity, internal audits, risk management, tax reporting, sanctions compliance, preservation of evidence, exercise or defense of legal claims, protection of KeySecure's legitimate interests, and other lawful operational, legal, regulatory, commercial, security, investigative, or business purposes.

21.2. Notwithstanding any request for deletion, erasure, restriction, withdrawal, or modification of Personal Data, KeySecure may retain, preserve, archive, or continue processing such information where deemed necessary or appropriate by KeySecure for purposes including but not limited to legal hold obligations, litigation preservation requirements, regulatory obligations, law enforcement cooperation, fraud prevention, cybersecurity purposes, dispute resolution, investigations, enforcement activities, audit requirements, sanctions compliance, compliance reviews, internal risk management, business continuity, or compliance with Applicable Laws.

21.3. Users further acknowledge and agree that blockchain records, distributed ledger records, backup systems, archived materials, decentralized networks, third-party systems, and external infrastructure may retain information independently of KeySecure and may be immutable, irreversible, publicly accessible, or incapable of deletion or modification. Accordingly, KeySecure does not represent, warrant, or guarantee that deleted information, Personal Data, blockchain records, transaction records, or related information will be permanently removed, erased, anonymized, or rendered inaccessible from all systems, backups, archives, blockchain networks, decentralized systems, third-party systems, or external infrastructure.

22. Data Security

22.1. KeySecure maintains and implements commercially reasonable administrative, technical, physical, organizational, operational, and cybersecurity safeguards designed to protect Personal



Data and related information against accidental, unlawful, unauthorized, fraudulent, malicious, or improper access, collection, use, disclosure, alteration, destruction, loss, theft, corruption, compromise, misuse, exfiltration, interception, or processing. Such safeguards may include encryption technologies, authentication controls, wallet security infrastructure, access control procedures, cybersecurity protections, network security measures, operational security controls, monitoring systems, fraud detection systems, intrusion detection mechanisms, incident response procedures, risk management controls, system segregation measures, logging systems, internal governance controls, and other security measures deemed appropriate by KeySecure in its sole discretion.

22.2. Notwithstanding the foregoing, Users expressly acknowledge and agree that no transmission method, storage platform, cybersecurity framework, blockchain infrastructure, internet-based service, telecommunications network, cloud environment, distributed ledger system, or technological system can be guaranteed to be fully secure, uninterrupted, error-free, immune from unauthorized access, or completely protected against cyberattacks, hacking incidents, malware infections, ransomware attacks, phishing attacks, data breaches, technological failures, operational disruptions, or cybersecurity incidents. Accordingly, KeySecure makes no representation, warranty, guarantee, or undertaking whatsoever regarding absolute security, uninterrupted operation, or complete protection of Personal Data, Crypto Assets, accounts, devices, systems, communications, or related information.

22.3. Users acknowledge and agree that no technological system, blockchain infrastructure, cybersecurity framework, transmission method, storage system, decentralized network, or internet-based platform can be guaranteed to be completely secure, immune from compromise, or entirely free from vulnerabilities, interruptions, cyberattacks, unauthorized access, operational failures, or technological risks, and KeySecure shall not guarantee absolute security of Personal Data, Crypto Assets, accounts, systems, communications, or related information.

23. Automated Decision-Making and Profiling

23.1. KeySecure may utilize automated systems, algorithms, artificial intelligence systems, machine learning technologies, blockchain analytics tools, behavioral analytics systems, fraud detection systems, sanctions screening systems, profiling tools, cybersecurity technologies, automated monitoring systems, and automated decision-making technologies in connection with fraud prevention, transaction monitoring, sanctions screening, anti-money laundering compliance, cybersecurity monitoring, investigations, operational security, risk scoring, account reviews, compliance assessments, suspicious activity monitoring, dispute resolution, enforcement activities, transaction approvals, account restrictions, and other lawful operational, compliance, legal, security, regulatory, or business purposes deemed necessary or appropriate by KeySecure.

23.2. Users expressly acknowledge and agree that such automated processing, profiling, monitoring, analytics, scoring, or decision-making activities may result in decisions, restrictions, actions, or outcomes affecting account access, transaction approvals, transaction delays, account suspensions, transaction restrictions, risk classifications, fraud determinations, compliance reviews, enhanced due diligence requirements, continued access to the Services, or other operational or compliance-related outcomes. KeySecure reserves the unrestricted right to rely



upon such automated systems and technologies in exercising its rights, obligations, compliance measures, risk management functions, operational decisions, and enforcement activities in connection with the Services.

- 23.3.** Where required under Applicable Laws, Users may have the right to request additional information regarding certain automated decision-making activities or request human review of certain decisions made solely through automated processing, subject to legal, operational, fraud prevention, cybersecurity, compliance, or regulatory limitations permitted under Applicable Laws.

24. Biometric Data

- 24.1.** Where permitted, authorized, or not prohibited under Applicable Laws, KeySecure may collect, receive, process, analyze, verify, store, monitor, transfer, disclose, and otherwise handle biometric information, biometric identifiers, facial recognition data, liveness detection data, selfie verification data, voice authentication information, behavioral biometric information, and related identity verification information for purposes including but not limited to identity verification, fraud prevention, authentication, anti-money laundering compliance, cybersecurity protection, account security, operational security, investigations, compliance reviews, enforcement activities, and other lawful operational, compliance, legal, security, or business purposes deemed necessary or appropriate by KeySecure.

- 24.2.** By accessing or using the Services and voluntarily providing such information, Users expressly acknowledge, consent, and agree to the collection, processing, analysis, verification, storage, transfer, disclosure, and retention of such biometric information in accordance with this Privacy Policy and Applicable Laws.

25. Cookies and Tracking Technologies

- 25.1.** KeySecure may utilize cookies, software development kits (SDKs), pixels, web beacons, advertising identifiers, local storage technologies, analytics tools, session tracking technologies, device fingerprinting technologies, behavioral analytics technologies, telemetry systems, and similar tracking, monitoring, analytics, or identification technologies for purposes including authentication, fraud prevention, cybersecurity protection, analytics, personalization, performance measurement, operational functionality, service optimization, behavioral analysis, machine learning, marketing, compliance monitoring, security monitoring, operational administration, and other lawful operational, commercial, compliance, legal, security, or business purposes.

- 25.2.** Users may configure browser settings or device settings to reject or restrict certain cookies or tracking technologies; however, Users acknowledge and agree that certain features, functionalities, services, operational capabilities, authentication mechanisms, or security protections of the Services may become unavailable, impaired, restricted, degraded, or non-functional as a result.

- 25.3.** Where required under Applicable Laws, KeySecure may request Users' consent for the use of certain cookies, tracking technologies, advertising technologies, analytics technologies, or similar technologies.



26. User Rights

26.1. Subject to Applicable Laws and any limitations, exemptions, restrictions, conditions, operational requirements, compliance obligations, fraud prevention measures, cybersecurity considerations, legal proceedings, investigations, law enforcement cooperation obligations, or legitimate business interests applicable thereto, Users may have certain rights relating to their Personal Data, including rights to:

- a. request access to Personal Data;
- b. request correction, rectification, or updating of inaccurate or incomplete Personal Data;
- c. request deletion or erasure of Personal Data;
- d. request restriction of processing activities;
- e. object to certain processing activities;
- f. request portability of Personal Data;
- g. withdraw consent where processing is based upon consent;
- h. request information relating to processing activities;
- i. request review of certain automated decision-making activities; and
- j. lodge complaints with competent data protection supervisory authorities.

26.2. KeySecure may require Users to verify their identity, authority, account ownership, request validity, or other relevant information before responding to any request relating to Personal Data.

26.3. Users acknowledge and agree that such rights may be limited, restricted, denied, deferred, or subject to conditions where necessary or appropriate for compliance with Applicable Laws, anti-money laundering obligations, fraud prevention, cybersecurity purposes, legal proceedings, investigations, dispute resolution, law enforcement cooperation, enforcement activities, regulatory obligations, operational requirements, internal risk management, preservation of evidence, protection of legitimate business interests, or other lawful purposes permitted under Applicable Laws. KeySecure reserves the unrestricted right to decline, restrict, defer, condition, or refuse any request relating to Personal Data where permitted or required under Applicable Laws.

27. Monitoring and Recording

27.1. Users expressly acknowledge and agree that communications, account activities, transactions, authentication activities, blockchain activities, customer support interactions, operational interactions, device activities, access records, transaction histories, communications data, and use of the Services may be monitored, intercepted, screened, reviewed, analyzed, recorded, processed, preserved, archived, retained, disclosed, and otherwise handled by KeySecure for purposes including compliance, fraud prevention, cybersecurity protection, operational administration, quality assurance, investigations, dispute resolution, enforcement activities, training, legal proceedings, regulatory cooperation, sanctions compliance, anti-money laundering obligations, internal audits, risk management, operational security, and other lawful operational, legal, regulatory, compliance, security, or business purposes deemed necessary or appropriate by KeySecure.

28. Third-Party Services Disclaimer



28.1. KeySecure does not own, control, operate, supervise, or administer third-party websites, blockchain networks, decentralized systems, custodians, merchants, payment processors, exchanges, banking partners, card issuers, telecommunications providers, cloud providers, infrastructure providers, or external platforms accessible through, integrated with, or connected to the Services. Accordingly, KeySecure shall not be responsible or liable whatsoever for the privacy practices, data handling activities, cybersecurity measures, operational activities, content, security controls, data protection standards, processing activities, availability, functionality, acts, omissions, failures, or conduct of any such third parties or external systems.

28.2. Users acknowledge and agree that access to and use of third-party services, websites, systems, platforms, protocols, blockchain networks, or external infrastructure shall be undertaken entirely at the User's own risk and subject to the applicable terms, conditions, policies, and practices of such third parties.

29. Minors

29.1. The Services are not directed to, intended for, designed for, or made available to individuals under eighteen (18) years of age or the applicable legal age of majority in the relevant jurisdiction. Users represent, warrant, and undertake that they possess the legal capacity, authority, and eligibility required to access and use the Services under Applicable Laws.

29.2. KeySecure reserves the unrestricted right, at any time and without prior notice, to suspend, restrict, terminate, freeze, deactivate, or close any account suspected, believed, or determined by KeySecure to belong to, be controlled by, or be used for the benefit of a minor or person lacking legal capacity.

30. Data Breach Response

30.1. In the event of any cybersecurity incident, unauthorized access event, hacking incident, data breach, security compromise, malware attack, ransomware incident, operational disruption, technological compromise, or other incident involving or potentially involving Personal Data, KeySecure may take such actions, measures, procedures, responses, or remediation activities as KeySecure deems necessary, appropriate, advisable, or desirable in its sole discretion to investigate, assess, contain, mitigate, remediate, respond to, monitor, report, recover from, document, or otherwise address such incidents in accordance with Applicable Laws, internal policies, operational requirements, cybersecurity protocols, regulatory expectations, or legitimate business interests.

31. Amendments

31.1. KeySecure reserves the unrestricted right, at any time and in its sole and absolute discretion, to amend, revise, supplement, restate, replace, modify, update, or otherwise change this Privacy Policy, in whole or in part, without prior notice, consent, or liability. Updated versions of this Privacy Policy may be published, communicated, or otherwise made available electronically through the Platform, mobile applications, website postings, APIs, email communications, or other electronic means determined by KeySecure.



- 31.2.** Users acknowledge and agree that continued access to or use of the Services following the publication, communication, or effectiveness of any revised Privacy Policy shall constitute acknowledgment and acceptance of the updated Privacy Policy.

32. Electronic Communications

- 32.1.** Users expressly consent to the electronic delivery, transmission, publication, provision, and receipt of privacy notices, disclosures, policies, records, communications, agreements, statements, reports, requests, responses, confirmations, notifications, and related materials through the Platform, mobile applications, APIs, email communications, website postings, push notifications, or other electronic means determined by KeySecure in its sole discretion.

- 32.2.** Users further acknowledge and agree that electronic communications shall have the same legal validity, enforceability, and evidentiary effect as physical written documents to the fullest extent permitted under Applicable Laws.

33. Jurisdiction-Specific Rights

- 33.1.** Users acknowledge and agree that certain rights, protections, disclosures, obligations, remedies, or restrictions described in this Privacy Policy may not apply in all jurisdictions and may be subject to limitations, exemptions, qualifications, restrictions, conditions, regulatory requirements, enforcement considerations, or lawful exceptions under Applicable Laws applicable in the relevant jurisdiction.

- 33.2.** Nothing contained in this Privacy Policy shall operate to grant, create, expand, or confer any rights, remedies, protections, or obligations beyond those required under Applicable Laws.

34. Relationship with Terms and Conditions

- 34.1.** This Privacy Policy forms an integral part of and shall be read together with the Terms and Conditions and any other policies, notices, guidelines, disclosures, rules, or terms issued by KeySecure from time to time, and certain provisions contained therein may apply to this Privacy Policy where applicable.

35. Inconsistency

- 35.1.** In the event of any inconsistency, conflict, ambiguity, discrepancy, or difference between this Privacy Policy and the Terms and Conditions, the Terms and Conditions shall prevail and govern to the fullest extent permitted under Applicable Laws where applicable, unless expressly stated otherwise.

36. Contact Information

For any questions, complaints, requests, inquiries, notices, or communications relating to this Privacy Policy, Personal Data processing activities, privacy rights, or data protection matters, Users may contact KeySecure through the following contact details:



Email: pay@keysecure.io

Website: <https://pay.keysecure.io/>