

Global Privacy Notice

Zivoe Labs Ltd. and applicable Zivoe entities

1 October 2026

1. Scope and who we are

This Global Privacy Notice (the “Notice”) explains how Zivoe Labs Ltd. and the Zivoe entity or entities identified for the relevant relationship (collectively, “Zivoe,” “we,” “us” or “our”) collect, use, disclose, retain, transfer and otherwise process information relating to an identified or identifiable natural person (“Personal Data”).

This Notice applies to Personal Data processed when you visit or use zivoe.com, app.zivoe.com or another Zivoe-operated website, application, portal or interface that links to this Notice; create or seek an account; complete KYC, KYB, accreditation, sanctions or eligibility checks; connect or verify a digital wallet; review, enter into or administer an Offering or financing relationship; communicate with us; attend an event; receive marketing from us; act for an investor, borrower, originator, service provider or other counterparty; or otherwise interact with Zivoe in a context where Zivoe determines the purposes and means of processing.

This Notice does not govern Personal Data processed solely by an independent controller under its own privacy notice, including a broker-dealer, bank, custodian, transfer agent, administrator, wallet provider, stablecoin issuer, blockchain network, identity-verification provider or other independent service when that party determines its own purposes and means. Where we act solely as a processor, service provider, contractor, data intermediary or similar role for another controller, the controller’s notice governs your relationship with that controller.

Zivoe Labs Ltd. is a British Virgin Islands company (company number 2154610). Postal address: Zivoe Labs Ltd., Trinity Chambers, PO Box 4301, Road Town, Tortola, British Virgin Islands. For privacy requests, contact legal@zivoe.com; inquire@zivoe.com is also available. The applicable Offering Documents or collection notice may identify an additional or different controller for a particular relationship.

References to a Zivoe entity include any lawful successor or permitted assignee resulting from a conversion, continuation, domestication, merger, reorganization, internal restructuring or permitted assignment, subject to applicable law. A corporate transaction does not eliminate statutory privacy rights.

2. Personal Data we collect

Category	Examples
Identity and contact	Name, date of birth where required, postal address, email, telephone number, username, account identifiers, photographs, signatures and similar identifiers.
Entity and authority	Employer or entity name, title, role, formation information, organizational documents, beneficial owners, control persons, authorized persons, powers or resolutions, and evidence of authority.
Verification and compliance	Government-issued identification, identity-document data, tax identifiers where required, nationality/citizenship/residence information, accreditation or professional-investor evidence, sanctions/PEP screening results, source-of-funds/source-of-wealth information, adverse-media or fraud indicators, and other KYC/KYB/AML/CFT information.
Financial and transaction	Bank or payment details, wallet addresses, blockchain transaction identifiers, investment/loan/participation instructions, holdings, transfers, funding, repayments, redemptions, distributions, balances, valuations, tax information and transaction history.
Credit / underwriting	Where applicable: borrower, guarantor, owner or obligor information; financial statements; receivables/portfolio data; creditworthiness and underwriting information; and consumer-report information only where lawfully obtained and a permissible purpose exists.
Technical and security	IP address, device and browser characteristics, operating system, session identifiers, authentication events, MFA events, approximate location inferred from IP, logs, security signals, cookies, SDKs, pixels and similar technologies.
Communications and records	Emails, calls, support requests, meeting notes, chat communications, recorded calls where lawfully permitted, consents, acknowledgments, electronic signatures, contract versions and audit evidence.

Category	Examples
Professional and business	Company, position, professional qualifications, business contact details, investment mandate, interests and information provided in diligence, partnership or vendor discussions.
Marketing and preferences	Event attendance, newsletter status, communication preferences, consent records, campaign interactions and permitted analytics.
Public / third-party information	Public registries, sanctions lists, professional sources, blockchain data, fraud/security databases, counterparties, service providers, referrals and other lawful third-party sources.
Sensitive / special-category	Only when necessary and lawful: government identifiers, financial-account credentials or information, precise location if deliberately collected, biometric identifiers if actually used, criminal-offence data where lawfully processed, and other data treated as sensitive under applicable law.

We do not request your wallet private key or seed phrase. Do not provide either to Zivoe. Public blockchain information may remain publicly available independently of Zivoe and may be practically impossible for Zivoe to erase from the underlying network.

3. Sources of Personal Data

- Directly from you, including forms, uploads, contracts, communications, wallet connections and transaction instructions.
- From your employer, entity, fund, adviser, authorized representative, beneficial owner, administrator, broker-dealer, bank, borrower, originator, servicer or other party involved in the relationship.
- From identity, accreditation, fraud, cybersecurity, sanctions, AML/CFT, blockchain-analytics and verification providers.
- From public records, corporate registries, court or regulatory records, professional sources, websites and public blockchain networks.
- From service providers operating our websites, infrastructure, communications, analytics and security tools, subject to applicable consent and opt-out requirements.
- From affiliates in accordance with applicable law and the purposes described in this Notice.

4. Why we process Personal Data

Purpose	What this may include
Provide and administer Services	Create and manage accounts; authenticate users; provide interfaces and support; maintain records; deliver documents; process instructions.
Offerings and transactions	Assess eligibility; execute and administer investments, loans, participations, redemptions, transfers, repayments and distributions; maintain registers and transaction records.
KYC/KYB, AML/CFT and sanctions	Verify identity and authority; identify beneficial owners; conduct sanctions, PEP, anti-fraud and anti-terrorist-financing screening; investigate suspicious activity; comply with reporting obligations.
Accreditation / investor classification	Verify accredited-investor, professional-investor, qualified-investor or other eligibility status where required.
Risk, underwriting and credit	Evaluate counterparties, borrowers, collateral, receivables, portfolios and transaction risk; monitor performance; detect deterioration or fraud; enforce contractual rights.
Security and integrity	Prevent, detect and investigate hacking, account takeover, malware, phishing, fraud, abusive activity, unauthorized transfers and other security incidents.
Legal and regulatory	Comply with securities, financial-services, tax, accounting, audit, sanctions, AML/CFT, recordkeeping, court, regulatory and lawful government obligations; establish, exercise or defend legal claims.
Operations and improvement	Administer infrastructure, monitor reliability, troubleshoot, perform analytics, improve workflows and product functionality, and conduct internal reporting.

Purpose	What this may include
Corporate transactions	Evaluate and complete financings, reorganizations, mergers, acquisitions, asset transfers or similar corporate transactions, subject to confidentiality and applicable law.
Communications	Respond to inquiries; provide account, security, compliance, transaction, reporting, servicing, legal and corporate-action notices.
Marketing and events	Send permitted newsletters, invitations and other promotional communications; measure engagement; manage preferences and consent.
Research / statistics	Create aggregated, de-identified or anonymized information where permitted, including operational, risk, portfolio and market analytics.

5. Lawful bases for EEA and UK processing

Where the EU GDPR or UK GDPR applies, Zivoe relies on one or more lawful bases appropriate to the specific processing. We do not use consent when another lawful basis is more appropriate merely to create the appearance of choice.

Basis	Typical use
Performance of a contract / steps at your request	Account administration, authenticated instructions, Offering or financing processes, support and other processing necessary to enter into or perform an agreement with you.
Legal obligation	KYC/AML/CFT, sanctions, tax, accounting, regulatory reporting, recordkeeping, court orders and other binding legal duties.
Legitimate interests	Fraud prevention, cybersecurity, network and platform security, business administration, due diligence, risk management, legal claims, product improvement, B2B communications and other interests that are not overridden by your rights and interests.
Consent	Optional marketing or nonessential cookies/tracking where consent is required; specific data uses where applicable law requires consent. Consent can be withdrawn prospectively.
Vital interests / public-interest grounds	Only where the law permits and the circumstances require them.

Where required, we will provide additional information about the legitimate interests relied upon, and we will honor applicable objections. We will not rely on legitimate interests to continue direct marketing to an EEA/UK individual after a valid objection to that marketing.

6. Special-category, sensitive and criminal-offence data

Zivoe seeks to minimize collection of sensitive Personal Data. Where such information is required for identity, fraud, sanctions, legal claims, employment or another lawful purpose, we process it only under an applicable legal condition and with appropriate safeguards. We do not infer sensitive characteristics for advertising. We do not use biometric information to uniquely identify a person unless that functionality is actually implemented, lawful, disclosed and supported by any required consent.

If a U.S. state privacy law provides a right to limit, opt out of, or consent to the processing of sensitive Personal Data, we will provide the required mechanism to the extent the processing is in scope and not exempt.

7. How we disclose Personal Data

We disclose Personal Data only as reasonably necessary for the purposes described in this Notice, as instructed or authorized by you, or as otherwise permitted or required by law. Recipients may include:

- Zivoe affiliates and special-purpose entities involved in the relevant relationship, subject to appropriate access controls and legal requirements.
- Identity, KYC/KYB, accreditation, sanctions, AML/CFT, fraud and blockchain-analytics providers.

- Administrators, servicers, custodians, transfer agents, broker-dealers, placement agents, banks, payment providers, stablecoin providers, wallet infrastructure providers and transaction counterparties.
- Cloud, hosting, cybersecurity, communications, data-room, document, analytics and other technology vendors.
- Auditors, accountants, tax advisers, insurers, consultants and legal counsel.
- Borrowers, originators, lenders, investors or counterparties where disclosure is necessary for a transaction and lawful.
- Governmental, regulatory, law-enforcement, judicial, arbitral and self-regulatory authorities where legally required or permitted.
- A buyer, investor, lender, successor or transaction participant in a financing, merger, acquisition, restructuring, reorganization or sale, subject to appropriate confidentiality and legal safeguards.

Some recipients act as processors or service providers for Zivoe; others may be independent controllers because they determine their own legal obligations and processing purposes. Their own privacy notices may apply.

8. Advertising, sale and sharing disclosures

Zivoe does not currently use Personal Data for targeted or cross-context advertising and does not deploy advertising pixels or audience-matching tools on the Services. Certain U.S. privacy laws define “sale” or “sharing” more broadly than a sale for money. If Zivoe later uses a technology or disclosure that constitutes a regulated sale or sharing, it will provide any legally required notice and opt-out mechanisms and honor applicable browser-based universal opt-out preference signals.

Zivoe currently uses only technologies necessary to operate, authenticate, secure and administer the Services. It does not currently deploy nonessential analytics or advertising cookies on the Services.

9. Cookies and similar technologies

We currently use only cookies, local storage, SDKs and similar technologies that are necessary to provide, authenticate, secure or administer the Services requested by the user. We do not currently use nonessential analytics or advertising cookies. If we introduce nonessential technologies later, we will identify their providers, purposes and durations and provide any notice, consent or choices required by applicable law before they are activated.

Strictly necessary technologies may remain active to support authentication, fraud prevention, cybersecurity, network management, transaction integrity and consent storage. If nonessential technologies are introduced, users will have any legally required means to reject them and later change or withdraw their choices. Privacy inquiries may be sent to legal@zivoe.com. Where a U.S. law provides an opt-out model, Zivoe will honor applicable opt-out rights and recognized universal opt-out signals to the extent required.

10. Direct marketing and communication preferences

Operational, transactional, security, legal, compliance, reporting, servicing and corporate-action communications are not optional marketing and may continue while the relevant relationship exists or as required by law.

Promotional communications are subject to separate preferences and applicable law. Where prior consent is required, we will obtain consent through a separate, specific and affirmative control. Marketing consent is not a condition of entering into an Offering or receiving a service unless the marketing itself is the requested service.

You may unsubscribe from promotional email by using the unsubscribe link or contacting legal@zivoe.com or inquire@zivoe.com. An objection or withdrawal applies prospectively and does not invalidate prior lawful processing.

11. Digital assets, wallets and public blockchains

A public blockchain is not controlled by Zivoe. Wallet addresses, transaction hashes, token transfers, smart-contract interactions and other data recorded on a public blockchain may be visible to the public, replicated across many nodes, transferred internationally and effectively immutable.

Zivoe may associate a wallet address or transaction with a verified account in its internal records for eligibility, sanctions, security, transfer-control, accounting, reporting or transaction-administration purposes. A request to erase internal Personal Data does not require or enable Zivoe to delete a public blockchain record that Zivoe does not control. Where legally required, we will instead consider measures such as deleting off-chain associations, restricting internal use, suppressing records from ordinary interfaces, or retaining only information required by law.

Do not send private keys, seed phrases or other credentials that would allow control of a wallet. Zivoe will not ask you to disclose a seed phrase.

12. Automated tools, analytics, AI and profiling

Zivoe may use automated or semi-automated tools for fraud detection, sanctions and blockchain screening, cybersecurity, identity verification, risk scoring, eligibility workflow, analytics and operational support. Human review may be used where appropriate.

If automated processing produces a decision with legal or similarly significant effects for you, applicable law may provide a right to information, human review, explanation, challenge or an opt-out. You may contact legal@zivoe.com about a decision or request a review where such a right applies.

This Notice does not authorize Zivoe to use Personal Data to train general-purpose artificial-intelligence models. Any such use must be separately reviewed, disclosed and supported by an applicable legal basis before implementation.

13. Consumer reports and the U.S. Fair Credit Reporting Act

This Section applies only if and to the extent Zivoe obtains, uses, furnishes or shares information subject to the U.S. Fair Credit Reporting Act ("FCRA") or Regulation V. Ordinary KYC/KYB, sanctions screening, business-credit diligence or public-record research does not automatically mean that Zivoe is using a "consumer report" for FCRA purposes.

Where Zivoe obtains a consumer report from a consumer reporting agency, Zivoe will obtain it only for a permissible purpose and will comply with applicable certification, notice, authorization, adverse-action, disposal, identity-theft and other requirements. If Zivoe furnishes information to consumer reporting agencies, applicable accuracy, dispute and furnishing requirements will be addressed in separate procedures.

If Zivoe or an affiliate uses certain eligibility information received from an affiliate to make marketing solicitations and the FCRA affiliate-marketing rule applies, the affected consumer will receive the applicable notice and a reasonable opportunity to opt out, subject to statutory exceptions.

Consumer-report information that is subject to the FCRA may be excluded from some state-privacy-law rights to the extent provided by those laws; other Personal Data concerning the same individual may remain subject to applicable state privacy rights.

14. U.S. financial privacy — GLBA / Regulation P

This Section applies only to the extent a Zivoe entity and a particular individual relationship are subject to the Gramm-Leach-Bliley Act ("GLBA") and Regulation P or another implementing privacy rule. Regulation P generally concerns nonpublic personal information about individuals obtaining financial products or services primarily for personal, family or household purposes; business or commercial relationships may fall outside that scope.

Where required, the covered Zivoe entity will provide a clear and conspicuous GLBA privacy notice at the time and in the form required by law, including the categories of information collected and disclosed, categories of affiliates and nonaffiliated third parties, and applicable confidentiality and security practices.

If a covered Zivoe entity discloses nonpublic personal information to a nonaffiliated third party outside an applicable statutory exception and an opt-out is required, the entity will provide a reasonable means to opt out before the disclosure. A GLBA opt-out does not apply to disclosures that law permits without opt-out, including certain disclosures necessary to process or service a transaction, protect against fraud, comply with law, or perform other functions covered by statutory exceptions.

This global Notice is not a substitute for the standardized Regulation P model privacy form where the model form is selected or a separate GLBA notice is otherwise required.

15. Security

We maintain administrative, technical and physical safeguards designed to protect Personal Data against unauthorized access, acquisition, use, disclosure, alteration, destruction or loss. Measures may include role-based access, encryption in transit and at rest where appropriate, authentication controls, logging and monitoring, vendor risk management, incident-response procedures, backups, network protections and employee confidentiality obligations.

No system, blockchain, network or method of transmission is completely secure. Security safeguards reduce risk but cannot guarantee that an unauthorized event will never occur.

Where a Zivoe entity is subject to the GLBA Safeguards Rule or another information-security rule, compliance depends on the entity's written information-security program and operational controls; this Notice does not itself satisfy those program requirements.

16. Data retention and deletion

We retain Personal Data only as long as reasonably necessary for the purposes for which it was collected, to maintain the relationship, and to satisfy applicable legal, regulatory, tax, accounting, audit, AML/KYC, sanctions, securities, contractual, security and recordkeeping obligations, establish or defend legal claims, resolve disputes, and enforce agreements.

Retention periods vary by data category and jurisdiction. Where practical and lawful, we delete, de-identify or anonymize Personal Data after the applicable retention period ends. Litigation holds, investigations, legal obligations and immutable public-blockchain records may prevent deletion or require longer retention.

Backups may retain information for a limited period until overwritten or securely retired, provided the information is not restored to active use except for disaster recovery, security or legally permitted purposes.

17. International transfers

Zivoe operates across jurisdictions and may process Personal Data in the British Virgin Islands, United States and other countries where Zivoe entities or service providers operate. Those countries may have privacy laws different from the laws where you live.

Where applicable law restricts international transfers, we use an approved transfer mechanism or another lawful basis. This may include adequacy decisions, European Commission Standard Contractual Clauses, a UK international data-transfer mechanism, contractual or organizational safeguards designed to provide comparable protection under Singapore law, reasonable steps required under Australian law, or another mechanism recognized by the relevant jurisdiction.

Where required, you may request information about the safeguards used for a restricted transfer by contacting inquire@zivoe.com. Some details may be redacted to protect confidential or security-sensitive information.

18. Your privacy rights and how to exercise them

Depending on where you live, the law that applies, the capacity in which you interact with Zivoe and the type of data involved, you may have some or all of the following rights:

Right	Summary
Access / know	Request confirmation of processing and access to Personal Data; in some jurisdictions, request categories, sources, purposes, recipients or specific pieces of information.
Correction	Request correction of inaccurate Personal Data.
Deletion / erasure	Request deletion of Personal Data, subject to legal, regulatory, contractual, security and other permitted exceptions.
Restriction	Ask that certain processing be restricted where the applicable law provides this right.
Portability	Receive certain Personal Data in a structured, commonly used, machine-readable format, or request transmission where legally available.
Object	Object to processing based on legitimate interests or to direct marketing where applicable.
Withdraw consent	Withdraw consent prospectively where processing relies on consent.
Opt out of sale / sharing / targeted advertising	Exercise applicable U.S. state rights, including through a recognized universal opt-out signal where required.
Limit sensitive-data use	Exercise a right to limit or withdraw consent for certain sensitive-data processing where applicable.

Right	Summary
Profiling / automated decisions	Opt out of, challenge or obtain information about qualifying automated decisions where applicable.
Appeal	Appeal a denial of a privacy request where applicable state law provides an appeal right.
Complaint	Complain to an applicable privacy, data-protection or regulatory authority.

Submit requests by email to inquire@zivoe.com or legal@zivoe.com. We may verify your identity and authority before acting on a request. We will use Personal Data provided for verification only for request handling, security and related legal obligations. Where permitted, an authorized agent may submit a request on your behalf, subject to verification of authority.

We do not discriminate against you for exercising applicable privacy rights. Exercising a right may affect our ability to provide a product or complete a transaction if the information is necessary for the requested service, KYC/AML, sanctions, eligibility, security, recordkeeping or another lawful purpose.

19. Children

The Services and Offerings are not directed to children. We do not knowingly offer investment or financing products through the Services to persons under 18 years of age. If we learn that we collected Personal Data from a child in circumstances requiring parental or guardian consent and no valid basis exists, we will take appropriate steps consistent with applicable law.

Jurisdictions may impose different age thresholds and consent requirements.

20. Changes to this Notice

We may update this Notice to reflect changes in law, technology, vendors, products, corporate structure or processing practices. We will post the effective date of the updated Notice and provide additional notice or obtain renewed consent where applicable law requires it. A change to this Notice does not retroactively create consent or waive statutory rights.

21. Contact and complaints

Privacy inquiries and rights requests: legal@zivoe.com; inquire@zivoe.com is also available. Postal address: Zivoe Labs Ltd., Trinity Chambers, PO Box 4301, Road Town, Tortola, British Virgin Islands.

If you are entitled to complain to a supervisory or privacy authority, you may do so in the jurisdiction provided by applicable law. We encourage you to contact us first so that we can try to address the issue.

JURISDICTION-SPECIFIC SUPPLEMENTS

These supplements apply only where the stated law applies to the relevant person and processing. They supplement, and do not reduce, the global protections above.

A. European Economic Area — GDPR Supplement

Where Regulation (EU) 2016/679 ("GDPR") applies, the controller is the Zivoe entity identified at collection or in the applicable transaction documents. EEA privacy requests may be sent to legal@zivoe.com.

- **Transparency.** We provide the identity and contact details of the controller; purposes and lawful bases; legitimate interests where applicable; recipients or categories of recipients; transfer safeguards; retention period or criteria; statutory/contractual nature of required data; rights; complaint rights; source information where data was not obtained directly; and required information about qualifying automated decision-making.
- **Rights.** Subject to conditions and exceptions, individuals may access, rectify, erase, restrict, port, object, withdraw consent, and complain to a supervisory authority.
- **Direct marketing.** You may object at any time to processing of Personal Data for direct marketing. Once a valid objection applies, we will stop processing your Personal Data for that direct-marketing purpose.
- **International transfers.** Restricted transfers will use a lawful GDPR transfer mechanism, such as an adequacy decision or appropriate safeguards including the European Commission's Standard Contractual Clauses where suitable.

- Automated decisions. If a solely automated decision produces legal or similarly significant effects, any applicable Article 22 rights and safeguards will be observed.

EEA supervisory authority: you may complain to the competent supervisory authority in your Member State of habitual residence, place of work or alleged infringement, subject to the GDPR.

B. United Kingdom — UK GDPR / PECR Supplement

Where UK data-protection law applies, references to GDPR rights and principles should be read together with the UK GDPR and Data Protection Act 2018, as amended. UK-specific transfer mechanisms will be used where required.

- Nonessential cookies and similar storage/access technologies will require consent where PECR requires consent. Strictly necessary exemptions are applied narrowly.
- Unsolicited electronic marketing to individual subscribers will be sent only where permitted by PECR, including valid consent or an applicable statutory exception. Consent requests will be separate from general terms and capable of withdrawal.
- UK privacy requests may be sent to legal@zivoe.com.
- You may complain to the UK Information Commissioner's Office where you have that right.

C. United States — State Privacy Supplement

This Section applies to residents of U.S. states with comprehensive consumer-privacy laws only to the extent the relevant law applies to Zivoe and the Personal Data at issue. Financial-services, GLBA-regulated information, FCRA-regulated information, entity-level, institutional-investor, B2B and other exemptions differ by state.

- Where required, residents may request access/confirmation, correction, deletion and portability.
- Where required, residents may opt out of sale, sharing, targeted advertising and qualifying profiling, and may appeal certain request denials.
- Where required, Zivoe will obtain consent before processing certain sensitive Personal Data or will provide a right to limit or opt out.
- Zivoe will honor recognized universal opt-out preference signals, including Global Privacy Control, to the extent applicable law requires the signal to be treated as a valid opt-out.
- Zivoe will not discriminate against a person for exercising a covered privacy right.

California

If the California Consumer Privacy Act, as amended (CCPA), applies to the relevant Personal Data, a California resident may have rights to know or access, delete, correct, opt out of sale or sharing, limit certain uses or disclosures of sensitive Personal Information, and receive nondiscriminatory treatment. If Zivoe sells or shares Personal Information as defined by the CCPA, Zivoe will provide the required opt-out method and honor Global Privacy Control where required.

Certain information subject to the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, or another statutory exemption may be outside some CCPA requirements. The applicable treatment depends on the data and the Zivoe entity processing it.

D. Hong Kong — PDPO Supplement

Where the Hong Kong Personal Data (Privacy) Ordinance ("PDPO") applies, Zivoe will collect Personal Data for lawful purposes directly related to its functions or activities, limit collection to what is necessary and not excessive, take practicable steps regarding accuracy, retention and security, and use Personal Data only for the disclosed purpose or a directly related purpose unless a lawful basis for another use exists.

At or before collection where required, additional information will identify whether providing data is obligatory or voluntary, the consequences of not providing required data, purposes of use, classes of transferees, and the contact route for access and correction.

Direct marketing: where the PDPO direct-marketing provisions apply, Zivoe will provide the required information and response channel and obtain the legally required consent or indication of no objection before using Personal Data for direct marketing. You may require Zivoe to cease using your Personal Data for direct marketing at any time without charge.

Access and correction requests may be submitted to inquire@zivoe.com or legal@zivoe.com.

E. Singapore — PDPA Supplement

Where Singapore's Personal Data Protection Act ("PDPA") applies, Zivoe will address applicable notification, consent, purpose-limitation, access and correction, accuracy, protection, retention, transfer-limitation, breach-notification and accountability obligations.

- You may withdraw consent that you previously gave or were deemed to give, subject to reasonable notice and legal consequences. We will explain likely consequences where required. Withdrawal does not prevent processing that is required or authorized without consent by law.
- You may request access to Personal Data and information about its use or disclosure, and may request correction, subject to applicable exceptions.
- Personal Data transferred outside Singapore will be protected in accordance with applicable transfer-limitation requirements, including measures designed to provide a standard of protection comparable to the PDPA.
- Zivoe will cease retaining Personal Data or remove the means by which it can be associated with particular individuals when retention is no longer needed for a legal or business purpose, subject to applicable requirements.

For Singapore privacy inquiries, contact legal@zivoe.com or inquire@zivoe.com.

F. Australia — Privacy Act / APP Supplement

Where the Australian Privacy Act 1988 and Australian Privacy Principles ("APPs") apply, Zivoe will maintain an up-to-date privacy policy, provide required collection notices, take reasonable steps regarding data quality and security, provide applicable access and correction rights, and address overseas disclosures in accordance with APP 8.

Direct marketing: where APP 7 applies, Zivoe will provide a simple means to opt out and will honor an opt-out request. Other Australian marketing laws, including the Spam Act and Do Not Call Register regime, may separately apply depending on the communication.

Automated decisions: Additional Australian privacy-policy transparency requirements concerning certain computer-program decisions commence on 10 December 2026 where the statutory conditions are met.

G. Japan — APPI Supplement

Where Japan's Act on the Protection of Personal Information ("APPI") applies, Zivoe will identify or notify purposes of use as required, handle retained personal data and third-party disclosures in accordance with applicable rules, respond to applicable individual requests, and satisfy requirements for cross-border transfers where applicable.

Any additional Japanese notice or cross-border transfer information required for a particular activity will be provided at or before collection.

H. Republic of Korea — PIPA Supplement

Where Korea's Personal Information Protection Act ("PIPA") applies, Zivoe will provide a localized privacy policy containing the elements required by PIPA, including applicable processing purposes, data items, retention, third-party provision and processing entrustment, cross-border transfers, rights procedures, security and responsible contact information.

Cross-border transfers involving Korean data subjects are subject to applicable PIPA requirements. Depending on the transfer, those requirements may include a particular legal basis, notice and separate consent.

Individuals may have rights including access, correction, deletion and suspension of processing, subject to applicable law. Korean privacy requests may be sent to legal@zivoe.com.

I. Other APAC and other jurisdictions

Privacy laws in other Asia-Pacific jurisdictions may provide additional rights, notices or safeguards. Contact legal@zivoe.com with a request relating to one of those jurisdictions.

The same approach applies to Latin America, Canada, the Middle East and other regions not specifically addressed above.

