Veltrano Solutions Ltd. Privacy Policy

This Privacy Policy includes important information about your personal data and we encourage you to read it carefully.

Welcome

Veltrano Solutions Ltd. ("Veltrano," "we," "our," or "us") is a global fraud asset recovery establishment specializing in the investigation, tracing, and recovery of misappropriated digital and traditional assets. We provide forensic investigation services, asset tracing, legal support coordination, and recovery solutions to individuals, corporate entities, law enforcement agencies, and institutional clients affected by financial fraud, cybercrime, and asset misappropriation.

This Privacy Policy ("Policy") describes the Personal Data that we collect, how we use and share it, and how you can reach us with privacy-related inquiries. The Policy also outlines your rights and choices as a data subject, including the right to object to certain uses of your Personal Data.

Depending on the engagement, Veltrano assumes the role of a "data controller" and/or "data processor" (or "service provider"). For more details about our privacy practices, including our role, the specific Veltrano entity responsible under this Policy, and our legal bases for processing your Personal Data, please visit our Privacy Center.

Defined Terms

In this Policy, "Veltrano," "we," "our," or "us" refers to the Veltrano entity responsible for the collection, use, processing, and handling of Personal Data as described in this

document. Depending on your jurisdiction, the specific Veltrano entity responsible for your Personal Data might vary.

"Personal Data" refers to any information associated with an identified or identifiable individual, which can include data that you provide to us, and that we collect about you during your interaction with our Services (such as device information, IP address, financial transaction records, etc.).

"Services" refers to the products, services, and applications that we provide under the Veltrano Services Agreement or other applicable terms of service (collectively, "Professional Services"), including forensic investigation, asset tracing, fraud analysis, legal support coordination, and recovery services; our websites ("Sites") such as Veltrano.com; client portals; and other Veltrano applications and online services. We provide Professional Services to entities ("Clients"). We may also provide direct services to individuals ("Direct Users").

"Recovery Partners" are financial institutions, law enforcement agencies, legal firms, cybersecurity partners, blockchain analytics providers, forensic accountants, and other specialized partners that we collaborate with, directly or indirectly, to provide the Services.

"Investigation Data" refers to data collected or used by Veltrano in relation to fraud investigations and asset recovery efforts. Some Investigation Data is Personal Data and may include: your name, email address, contact number, residential and business addresses, financial account information (bank accounts, cryptocurrency wallets, investment accounts), transaction history, digital forensics data, IP addresses, device identifiers, communication records, legal documentation, identity verification documents (passports, driver's licenses, government IDs), employment information, corporate ownership structures, and case-related correspondence.

Depending on the context, "you" might be a Direct User, Client Representative, Third Party Subject, or Visitor:

- Direct Users. When you engage Veltrano directly for personal fraud recovery services, such as when you are a victim of identity theft, investment fraud, or cybercrime, we refer to you as a "Direct User."
- Client Representatives. When you are acting on behalf of an existing or potential Client—perhaps as a corporate officer, legal counsel, compliance officer, or authorized agent—we refer to you as a "Client Representative."
- Third Party Subjects. When your Personal Data is involved in an investigation or recovery matter but you are not the Client or Direct User requesting our services (for example, when you are a suspected fraudster, witness, or associated party in a case we are investigating), we refer to you as a "Third Party Subject."
- Visitors. When you interact with Veltrano by visiting a Site without being logged into a Veltrano account, or when your interaction with Veltrano does not involve you being a Direct User, Client Representative, or Third Party Subject, or when you visit a Veltrano office or other Veltrano premises, we refer to you as a "Visitor."

Table of Contents

Our collection and use of Personal Data differs based on whether you are a Direct User, Client Representative, Third Party Subject, or Visitor, and the specific Service that you are using. For example, if you're a corporate compliance officer engaging us for fraud investigation services, we may collect your Personal Data to onboard your organization; at the same time, you might also be a Third Party Subject if your information appears in another Client's investigation matter.

1.1 Direct Users

We provide Professional Services directly to individuals who have been victims of fraud or asset misappropriation. Additional details regarding our collection, use, and sharing of Direct User Personal Data, including the legal bases we rely on for processing such data, can be found in our Privacy Center.

a. Personal Data we collect about Direct Users

Fraud Recovery Engagement. When you engage Veltrano to investigate fraud or recover assets on your behalf, we collect comprehensive Personal Data necessary to pursue your case. This includes your full name, contact information, government-issued identification, financial account details (bank accounts, cryptocurrency wallets, investment portfolios), transaction histories, communication records with suspected fraudsters, contracts and agreements, evidence of fraudulent activity, and any other documentation relevant to your case.

Identity Verification and KYC. We are required by law and our professional obligations to verify your identity before commencing services. We collect identity documents (passport, driver's license, national ID), proof of address, biometric data (for facial recognition matching when required), and may conduct background checks to comply with anti-money laundering (AML) regulations and prevent conflicts of interest.

Financial Account Monitoring. With your authorization, we may collect ongoing financial data from your accounts to trace fund flows, identify recovery opportunities, and monitor for continued fraudulent activity. This includes account balances, transaction details, counterparty information, and metadata associated with financial transfers.

Digital Forensics Data. When investigating cyber fraud or digital asset theft, we may collect device information, IP addresses, digital wallet addresses, blockchain transaction data, email headers, social media activity, and other digital artifacts relevant to tracing stolen assets.

Communication and Case Management. We collect all correspondence related to your case, including emails, phone call recordings, video conference data, chat logs, and documentation shared through our secure client portal.

More. For further information about other types of Personal Data that we may collect about Direct Users, including about your online activity and your engagement with our Services, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Direct Users' Personal Data

Service Provision. We use and share your Personal Data to provide the Professional Services to you, which includes forensic investigation, asset tracing, legal coordination, recovery operations, case management, and communication about your matter. For example, Veltrano may use your financial data to trace stolen funds across banking networks or blockchain ledgers.

Recovery Partners and Legal Coordination. To recover your assets, we must share your Personal Data with Recovery Partners, including:

- Law Enforcement Agencies: We share Investigation Data with police, financial crime units, cybercrime divisions, and regulatory authorities to support criminal investigations and recovery efforts.
- Legal Professionals: We share case information with law firms, barristers, and legal advisors coordinating recovery litigation or arbitration on your behalf.
- Financial Institutions: We share relevant data with banks, payment processors, cryptocurrency exchanges, and financial service providers to freeze accounts, reverse transactions, or secure recovered assets.
- Forensic Specialists: We share technical data with cybersecurity firms, blockchain analytics providers, digital forensics experts, and forensic accountants to trace and recover assets.

Fraud Prevention and Security. We use your Personal Data collected across our Services to detect fraud patterns, prevent further losses, and enhance our security protocols. We

may share anonymized or aggregated fraud indicators with industry partners and law enforcement to combat financial crime.

Regulatory Compliance. We use and share your Personal Data to comply with legal obligations, including AML regulations, Know-Your-Customer (KYC) requirements, sanctions screening, suspicious activity reporting, and court orders.

Case Documentation and Evidence. We use your Personal Data to compile evidence packages for legal proceedings, insurance claims, regulatory filings, and law enforcement submissions.

More. For further information about ways we may use and share Direct Users' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

1.2 Client Representatives

Veltrano provides Professional Services to corporate Clients, financial institutions, and institutional entities. When acting as a service provider—also referred to as a Data Processor—for a Client, we process Personal Data in accordance with our agreement with the Client and the Client's lawful instructions.

Clients are responsible for ensuring that the privacy rights of their personnel and associated individuals are respected, including obtaining appropriate consents and making disclosures about their own data collection and use associated with their fraud prevention and asset recovery activities.

We provide more comprehensive information about our collection, use, and sharing of Client Representative Personal Data in our Privacy Center, including the legal bases we rely on for processing your Personal Data.

a. Personal Data we collect about Client Representatives

Engagement and Onboarding. When you register for Veltrano services on behalf of a Client, we collect your name, title, business contact information, corporate credentials, and authorization documentation to establish service relationships and verify your authority to engage our services.

Identification and Verification. As a Client Representative, we collect your government-issued identification, proof of corporate authority, beneficial ownership information, and may conduct due diligence checks to comply with AML regulations, sanctions screening, and our professional obligations.

Case Collaboration Data. During fraud investigations and asset recovery operations, we collect case-related communications, documentation you provide about affected parties, internal investigation reports, and coordination records with your organization's legal, compliance, and security teams.

Corporate Structure Information. We collect data about corporate ownership structures, beneficial owners, authorized signatories, and related party information necessary for asset tracing and recovery operations.

More. For further information about other types of Personal Data that we may collect about Client Representatives, including about your online activity, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Client Representatives' Personal Data

Professional Services Delivery. We use and share your Personal Data to deliver investigation services, asset tracing, recovery coordination, and case management to your organization.

Coordination with Recovery Partners. We share your contact and authorization information with Recovery Partners as necessary to execute recovery operations on

behalf of your organization, including law firms, financial institutions, and regulatory bodies.

Fraud Detection and Risk Management. We use your Personal Data to assess fraud risks associated with cases, verify identities, prevent conflicts of interest, and ensure compliance with professional standards.

Regulatory and Legal Compliance. We use and share your Personal Data to comply with AML, KYC, sanctions screening, and other legal obligations applicable to corporate fraud investigations.

More. For further information about additional ways in which we may use and share Client Representatives' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

1.3 Third Party Subjects

In the course of our Professional Services, we inevitably collect Personal Data about individuals who are not our Clients or Direct Users—such as suspected fraudsters, witnesses, associates, or counterparties in transactions. We refer to these individuals as "Third Party Subjects."

a. Personal Data we collect about Third Party Subjects

Investigation-Related Data. We collect Personal Data about Third Party Subjects from public records, open-source intelligence (OSINT), blockchain analysis, financial transaction data, social media, corporate registries, legal filings, and information provided by our Clients or Direct Users.

Identity and Location Data. We may collect names, aliases, contact information, addresses, government identification numbers, digital identifiers (IP addresses, device IDs, wallet addresses), biometric data (from images or video), and location data relevant to investigations.

Financial and Transaction Data. We collect bank account information, cryptocurrency wallet addresses, transaction histories, investment records, property ownership, and other financial data relevant to tracing misappropriated assets.

Associational and Network Data. We collect information about relationships, corporate affiliations, business networks, family connections, and other associational data relevant to understanding fraud schemes and asset flows.

More. For further information about other types of Personal Data that we may collect about Third Party Subjects, please see the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Third Party Subjects' Personal Data

Fraud Investigation and Asset Tracing. We use Third Party Subject Personal Data exclusively for legitimate fraud investigation, asset recovery, and legal compliance purposes. This includes tracing stolen assets, identifying concealment mechanisms, mapping criminal networks, and supporting legal proceedings.

Law Enforcement and Regulatory Sharing. We share Third Party Subject Personal Data with law enforcement agencies, regulatory authorities, and financial intelligence units to support criminal investigations, prosecutions, and regulatory actions.

Legal Proceedings. We share Third Party Subject Personal Data with courts, tribunals, arbitration panels, and legal professionals in connection with civil recovery litigation, asset freezing orders, and judgment enforcement.

Risk Prevention and Industry Cooperation. We may share anonymized or aggregated fraud pattern data with industry partners, financial institutions, and fraud prevention networks to combat financial crime, provided such sharing does not identify specific Third Party Subjects without legal basis.

More. For further information about additional ways we may use and share Third Party Subjects' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

1.4 Visitors

We collect, use, and share the Personal Data of Visitors. More details about how we collect, use, and share Visitors' Personal Data, along with the legal bases we rely on for processing such Personal Data, can be found in our Privacy Center.

a. Personal Data we collect about Visitors

Website and Online Interaction. When you browse our Sites, we receive your Personal Data, either provided directly by you or collected through our use of cookies and similar technologies. See our Cookie Policy for more information. If you opt to complete a form on the Site or third-party websites where our advertisements are displayed, we collect the information you included in the form. This may include your contact information and other information pertaining to your questions about our Services.

Office Visits and Events. When you visit our offices or other Veltrano premises or attend Veltrano events, we may collect registration information (including access requirements) and photo and audio-visual data captured on CCTV or other video systems for security purposes.

More. Further details about other types of Personal Data that we may collect from Visitors, including your online activity, can be found in the *More ways we collect, use, and share Personal Data* section below.

b. How we use and share Visitors' Personal Data

Personalization. We use the data we collect about you using cookies and similar technologies to measure engagement with the content on the Sites, improve relevancy and navigation, customize your experience (such as language preference and

region-specific content), and curate content about Veltrano and our Services that's tailored to you.

Marketing and Communications. Where permitted by applicable law, and where required with your consent, we use and share Visitors' Personal Data with third parties so we can advertise and market our Services. Subject to applicable law, including any consent requirements, we may advertise through interest-based advertising and track the efficacy of such ads. See our Cookie Policy.

Engagement. As you interact with our Sites, we use the information we collect about and through your devices to provide opportunities for further interactions, such as discussions about Services or interactions with chatbots, to address your questions.

More. For more information about additional ways we may use and share Visitors' Personal Data, please see the *More ways we collect, use, and share Personal Data* section below.

2. More ways we collect, use and share Personal Data

In addition to the ways described above, we also process your Personal Data as follows:

a. Collection of Personal Data

Online Activity. Depending on the Service used and how our Professional Services are implemented, we may collect information related to:

- The devices and browsers you use across our Sites and third-party websites, apps, and other online services ("Third-Party Sites").

- Usage data associated with those devices and browsers and your engagement with our Services, including data elements like IP address, plug-ins, language preference, time spent on Sites and Third-Party Sites, pages visited, links clicked, and the pages that led you to our Sites and Third-Party Sites.

Communication and Engagement Information. We also collect information you choose to share with us through various channels, such as support tickets, emails, or social media. If you respond to emails or surveys from Veltrano, we collect your email address, name, and any other data you opt to include in your email or responses. If you engage with us over the phone, we collect your phone number and any other information you might provide during the call. Calls with Veltrano or Veltrano representatives may be recorded and transcribed for quality assurance and legal compliance purposes.

Open Source Intelligence (OSINT). For fraud investigation purposes, we collect publicly available information from social media platforms, corporate registries, court records, news archives, academic publications, and other open sources relevant to our cases.

Third-Party Data Providers. We may obtain Personal Data from third-party data providers, including credit bureaus, corporate intelligence services, blockchain analytics firms, and public record databases, to support our investigation and verification activities.

b. Use of Personal Data

Besides the use of Personal Data described above, we use Personal Data in the ways listed below:

Analyzing, Improving, and Developing our Services. We collect and process Personal Data throughout our various Services to improve our investigation methodologies, develop new recovery techniques, and support our efforts to make our Services more efficient, relevant, and effective. We may use Personal Data to generate aggregate and statistical information to understand and explain fraud trends and recovery outcomes.

Artificial Intelligence and Machine Learning. We may use Personal Data to train artificial intelligence models to enhance our fraud detection capabilities, improve asset tracing algorithms, and automate pattern recognition in financial crimes, provided such use complies with applicable law and professional obligations.

Communications. We use the contact information we have about you to deliver our Services, which may involve sending authentication codes or case updates via SMS or email. We do not share mobile data we collect for authentication purposes with third parties for marketing or promotional purposes.

Fraud Prevention and Security. We collect and use Personal Data to help us identify and manage activities that could be fraudulent or harmful, secure our Services against unauthorized access, use, alteration or misappropriation of Personal Data, information, and funds. We collect information from publicly available sources, third parties, and via the Services we offer to verify identities and prevent fraud.

Compliance with Legal Obligations. We use Personal Data to meet our contractual and legal obligations related to anti-money laundering, Know-Your-Customer ("KYC") laws, anti-terrorism activities, sanctions screening, export control, and prohibition of doing business with restricted persons, among other legal obligations. We may monitor transaction patterns and other signals to identify fraud, money laundering, and other harmful activity.

Minors. Our Services are not directed to children under the age of 16, and we request that they do not provide Personal Data to seek Services directly from Veltrano. In certain jurisdictions, we may impose higher age limits as required by applicable law.

c. Sharing of Personal Data

Besides the sharing of Personal Data described above, we share Personal Data in the ways listed below:

Veltrano Affiliates. We share Personal Data with other Veltrano-affiliated entities for purposes identified in this Policy, including global case coordination and resource sharing.

Service Providers or Processors. In order to provide, communicate, market, analyze, and deliver our Services, we depend on service providers. These providers offer critical services such as providing cloud infrastructure, conducting analytics, verifying identities, identifying potentially harmful activity, and providing customer service and audit functions. We authorize these service providers to use or disclose the Personal Data we make available to them to perform services on our behalf and to comply with relevant legal obligations. We require these service providers to contractually commit to security and confidentiality obligations.

Recovery Partners. We share Personal Data with certain Recovery Partners to provide our Services, including law enforcement agencies, financial institutions, legal professionals, and forensic specialists as detailed throughout this Policy.

Others with Consent. In some situations, we may refer you to others (like specialized legal firms or forensic experts). In these instances, we will disclose the identity of the third party and the information to be shared with them, and seek your consent to share the information where required.

Corporate Transactions. If we enter or intend to enter a transaction that modifies the structure of our business, such as a reorganization, merger, sale, joint venture, assignment, transfer, change of control, or other disposition of all or part of our business, assets, or stock, we may share Personal Data with third parties in connection with such transaction.

Compliance and Harm Prevention. We share Personal Data when we believe it is necessary to comply with applicable law; to enforce our contractual rights; to secure and protect the Services, rights, privacy, safety, and property of Veltrano, you, Clients, and

others; and to respond to valid legal requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities.

3. Legal bases for processing Personal Data

For purposes of the General Data Protection Regulation (GDPR) and other applicable data protection laws, we rely on a number of legal bases to process your Personal Data. For some jurisdictions, there may be additional legal bases, which are outlined in the Jurisdiction-Specific Provisions section below.

a. Contractual and Pre-Contractual Business Relationships. We process Personal Data to enter into business relationships with prospective Clients and Direct Users and fulfill our respective contractual obligations with them. These processing activities include:

- Creation and management of Veltrano accounts and case files;
- Assessment of fraud matters and development of recovery strategies;
- Execution of investigation services, asset tracing, and recovery operations;
- Communication about case progress and service delivery.

b. Legal Compliance. We process Personal Data to verify identities, comply with obligations related to fraud monitoring, prevention, and detection, laws associated with identifying and reporting illicit and illegal activities (such as AML and KYC regulations), and professional reporting obligations. These legal obligations may require us to report our compliance to third parties and subject ourselves to regulatory audits.

c. Legitimate Interests. Where permitted under applicable law, we rely on our legitimate business interests to process your Personal Data, including:

- Detection, monitoring, and prevention of fraud and financial crimes;
- Mitigation of financial loss, claims, liabilities, or other harm to Clients, Direct Users, and Veltrano;

- Protection of our professional reputation and operational integrity;
- Improvement of our investigation methodologies and recovery techniques;
- Network and information security throughout Veltrano and our Services;
- Sharing of Personal Data with third party service providers that offer services on our behalf.

d. Consent. We may rely on consent or explicit consent to collect and process Personal Data regarding our interactions with you and the provision of our Services. When we process your Personal Data based on your consent, you have the right to withdraw your consent at any time.

e. Substantial Public Interest. We may process special categories of Personal Data when such processing is necessary for reasons of substantial public interest and consistent with applicable law, such as when we conduct investigations into serious financial crimes or support law enforcement in matters of significant public concern.

f. Vital Interests. We may process Personal Data when necessary to protect the vital interests of individuals or other persons, such as in emergency situations involving immediate financial harm or safety threats.

4. Your rights and choices

Depending on your location and subject to applicable law, you may have choices regarding our collection, use, and disclosure of your Personal Data:

a. Opting out of receiving electronic communications from us

If you wish to stop receiving marketing-related communications from us, you can opt-out by clicking the unsubscribe link included in such communications or by contacting us. We'll try to process your request(s) as quickly as reasonably practicable. However, even if

you opt out of receiving marketing-related communications, we retain the right to communicate with you about the Services you receive and important legal notices.

b. Your data protection rights

Depending on your location and subject to applicable law, you may have the following rights regarding the Personal Data we process about you as a data controller:

- The right to request confirmation of whether Veltrano is processing Personal Data associated with you;
- The right to request access to the Personal Data Veltrano processes about you;
- The right to request that Veltrano rectify or update your Personal Data if it's inaccurate or incomplete;
- The right to request that Veltrano erase your Personal Data in certain circumstances as provided by law;
- The right to request that Veltrano restrict the use of your Personal Data in certain circumstances;
- The right to request that we export the Personal Data we hold about you to another company, where technically feasible;
- The right to withdraw your consent if your Personal Data is being processed based on your consent;
- The right to object to the processing of your Personal Data if we are processing based on legitimate interests;
- The right not to be discriminated against for exercising these rights;
- The right to appeal any decision by Veltrano relating to your rights by contacting our Data Protection Officer.

c. Process for exercising your data protection rights

To exercise your data protection rights related to Personal Data we process as a data controller, visit our Privacy Center or contact us as outlined below. For Personal Data we process as a data processor on behalf of Clients, please reach out to the relevant Client to exercise your rights.

5. Security and Retention

We maintain organizational, technical, and administrative measures designed to protect the Personal Data covered by this Policy from unauthorized access, destruction, loss, alteration, or misuse. These measures include encryption, access controls, secure facilities, and regular security assessments. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure.

We retain your Personal Data for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, regulatory, tax, accounting, or reporting requirements. For fraud investigation matters, we typically retain case files and associated Personal Data for a minimum of seven years following case closure to comply with legal obligations, support potential future legal proceedings, and maintain records for regulatory compliance.

Even after we stop providing Services directly to you, we may continue to retain your Personal Data to:

- Comply with legal and regulatory obligations;
- Enable fraud monitoring, detection, and prevention activities;
- Comply with tax, accounting, and financial reporting obligations;
- Support potential future legal proceedings or regulatory inquiries;
- Maintain professional indemnity insurance and professional standards compliance.

6. International Data Transfers

As a global business, we transfer Personal Data to countries other than your own, including the United Kingdom, United States, European Union member states, and other jurisdictions where our Recovery Partners and service providers operate. These countries might have data protection regulations different from those in your country.

When transferring data across borders, we take measures to comply with applicable data protection laws. We employ appropriate safeguards such as:

- Transfers to countries recognized as having adequate data protection;

- EU Standard Contractual Clauses approved by the European Commission;
- UK International Data Transfer Addendum;
- Other lawful methods available under applicable law.

Veltrano complies with applicable data privacy frameworks and maintains certifications where required for international data transfers.

7. Updates and notifications

We may change this Policy from time to time to reflect new services or changes in our privacy practices or relevant laws. Any changes are effective when we post the revised Policy on the Services or otherwise provide notice as required by law.

We may provide you with disclosures and alerts regarding the Policy or Personal Data collected by posting them on our website and, where applicable, by contacting you through your account or registered contact information.

8. Jurisdiction-specific provisions

You may exercise your rights by contacting our Data Protection Officer at dpo@veltrano.com. If you are a resident of the EEA or UK and believe our processing contradicts the GDPR, you may direct complaints to the UK Information Commissioner's Office or your local supervisory authority.

United States. If you are a US consumer, we process your personal information in accordance with applicable federal and state privacy laws. You may have rights including:

- The right to know what personal information we collect, use, disclose, and sell;
- The right to delete personal information;
- The right to opt-out of the sale or sharing of personal information;
- The right to non-discrimination for exercising privacy rights;
- The right to correct inaccurate personal information.

We do not "sell" Personal Data as traditionally understood, but we may share data with service providers and partners as described in this Policy.

Canada. "Applicable law" includes PIPEDA and provincial privacy laws. Our Global Head of Privacy serves as our privacy officer. You may contact them at privacy@veltrano.com.

Australia. "Personal Data" includes "personal information" under the Privacy Act 1988. If dissatisfied with our handling of complaints, you may contact the Office of the Australian Information Commissioner.

Singapore. "Applicable law" includes the Personal Data Protection Act 2012. We may rely on "deemed consent" when you voluntarily provide personal data.

Other Jurisdictions. For jurisdiction-specific rights in Brazil, India, Japan, Switzerland, and other locations, please contact our Data Protection Officer or visit our Privacy Center.

9. Contact us

If you have questions about this Privacy Policy or wish to exercise your rights, please contact us:

Data Protection Officer

Email: dpo@veltrano.com

Postal Address: [Veltrano Solutions Ltd. Registered Address]

Privacy Center: https://veltrano.com/privacy-center

Client Support: support@veltrano.com

For law enforcement or regulatory inquiries: legal@veltrano.com