# VIA EASY PAY — PRIVACY POLICY

**Last Updated: April 15, 2026 Effective Date: April 15, 2026**

## 1. INTRODUCTION

This Privacy Policy ("Policy") describes how Dealing Media Inc. O/A Via Easy (Ontario Corporation #1000850342) and Via Easy Pay Inc. (Wyoming C-Corporation #2025-001627521) (collectively, "Via Easy Pay," "Company," "we," "us," "our") collect, use, disclose, retain, and protect your personal information when you access or use our website at viaeasypay.com, our browser-based wallet application, and any related applications, tools, or interfaces (collectively, the "Platform").

Via Easy Pay is committed to protecting your privacy and handling your personal information in accordance with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable Canadian provincial privacy legislation, applicable United States federal and state privacy laws (including the California Consumer Privacy Act as amended by the California Privacy Rights Act, the Illinois Biometric Information Privacy Act, the Texas Capture or Use of Biometric Identifier Act, and other applicable state laws), and all other applicable privacy and data protection laws.

**Via Easy Pay is a payment technology infrastructure provider. Via Easy Pay is not a bank or authorized deposit-taking institution. Via Easy Pay does not hold, control, or have access to your digital assets at any time.**

By accessing or using the Platform, you acknowledge that you have read and understood this Policy and consent to the collection, use, and disclosure of your personal information as described herein. If you do not agree with this Policy, you must immediately cease all use of the Platform.

## 2. PRIVACY OFFICER

Via Easy Pay has appointed a Privacy Officer responsible for overseeing compliance with this Policy and applicable privacy laws. If you have any questions, concerns, or complaints regarding the collection, use, or disclosure of your personal information, or if you wish to exercise any of your rights described in this Policy, please contact our Privacy Officer:

**Privacy Officer** Via Easy Pay Email: compliance@viaeasy.com

For Canadian residents, if you are not satisfied with our response to your privacy inquiry, you have the right to file a complaint with the Office of the Privacy Commissioner of Canada:

Office of the Privacy Commissioner of Canada 30 Victoria Street Gatineau, Quebec K1A 1H3 Toll-free: 1-800-282-1376 Website: www.priv.gc.ca

## 3. INFORMATION WE COLLECT

We collect the following categories of personal information in connection with the Platform and Services. The specific information collected depends on how you interact with the Platform and which features you use.

### 3.1 Identity Data

When you use the Platform, create a wallet, or access features that require identity verification, we may collect:

- Full legal name (first name, middle name, last name)
- Date of birth
- Government-issued identification number and document images (for KYC verification conducted by Third-Party Service Providers)
- Nationality and country of residence
- Email address
- Phone number
- Residential address
- Photograph or selfie image (for identity verification conducted by Third-Party Service Providers)

### 3.2 Biometric Data

**Please refer to Section 8 of this Policy for a dedicated, comprehensive disclosure regarding the collection and processing of Biometric Data. Please also refer to our standalone Biometric Privacy Disclosure available at viaeasypay.com/biometric-privacy.**

The Platform uses your device's native biometric authentication capabilities (such as Face ID, Touch ID, fingerprint recognition, or equivalent hardware-backed biometric systems) for wallet creation and transaction authorization. Via Easy Pay collects and processes biometric identifiers, including facial geometry data, for the purposes described in Section 8.

### 3.3 Transaction Data

When you conduct transactions through the Platform, we collect:

- Transaction type (send, receive, request, on-ramp, off-ramp)
- Transaction amount and currency denomination
- Blockchain wallet addresses (sender and recipient)
- Blockchain transaction hashes and confirmation status
- Payment Link identifiers and status (created, claimed, expired, returned)
- Timestamps of all transactions
- Network and chain identifiers
- Token type and standard

### 3.4 Device and Technical Data

When you access the Platform, we automatically collect:

- Device type, model, and operating system
- Browser type and version
- Screen resolution and device capabilities
- Biometric authentication capability indicators (whether your device supports Face ID, Touch ID, or equivalent — not the biometric data itself)
- Unique device identifiers
- Mobile network information
- Language and locale settings
- Hardware security module capabilities

### 3.5 Usage Data

We collect information about how you interact with the Platform, including:

- Pages and features accessed
- Actions taken on the Platform (clicks, navigation patterns)

- Time spent on the Platform and individual pages
- Referral source (how you arrived at the Platform)
- Frequency and recency of visits
- Feature usage patterns
- Error logs and performance data

**3.6 Network and Location Data**

- Internet Protocol (IP) address
- Approximate geographic location derived from IP address (city/region level — we do not collect precise GPS coordinates)
- Internet service provider
- Connection type and speed

**3.7 Communications Data**

If you contact us for support or other purposes, we collect:

- Content of your communications (emails, messages, support tickets)
- Contact information provided in communications
- Timestamps of communications
- Support ticket identifiers and resolution status

**3.8 Information from Third-Party Service Providers**

We may receive personal information about you from Third-Party Service Providers, including:

- Identity verification results from KYC providers
- Transaction data from on/off-ramp service providers
- Risk assessment and fraud screening results
- Sanctions and watchlist screening results
- Blockchain analytics data

## 4. HOW WE USE YOUR INFORMATION

We use your personal information for the following purposes. Under PIPEDA, we collect and use personal information only for purposes that a reasonable person would consider appropriate in the circumstances.

### 4.1 Provision of Services

- To facilitate the creation and operation of your Self-Custodial Wallet
- To process and facilitate transactions, including the generation and redemption of Payment Links
- To display your wallet balance and transaction history
- To enable biometric authentication for wallet access and transaction authorization
- To connect you with Third-Party Service Providers for On/Off-Ramp Services

### 4.2 Legal and Regulatory Compliance

- To comply with applicable anti-money laundering ("AML") and counter-terrorist financing ("CTF") laws and regulations, including the PCMLTFA and its regulations
- To conduct or facilitate identity verification (KYC) as required by applicable law
- To perform transaction monitoring and suspicious activity detection
- To comply with sanctions screening obligations under OFAC, SEMA, the Magnitsky Act, and other applicable sanctions regimes
- To file required reports with regulatory authorities, including FINTRAC
- To comply with the Travel Rule for virtual currency transfers at or above applicable thresholds
- To respond to lawful requests from law enforcement and regulatory authorities
- To maintain records as required by applicable law (including the 5-year retention requirement under FINTRAC regulations)

### 4.3 Security and Fraud Prevention

- To detect, prevent, investigate, and report fraud, unauthorized access, and other illegal or suspicious activity
- To protect the security and integrity of the Platform
- To verify user identity and prevent impersonation

- To enforce our Terms of Service and Acceptable Use Policy
- To conduct risk assessments

### 4.4 Platform Improvement

- To understand how users interact with the Platform
- To identify and resolve technical issues, bugs, and errors
- To develop, test, and improve new and existing features
- To conduct internal analytics and reporting
- To optimize Platform performance and user experience

### 4.5 Communications

- To respond to your inquiries and support requests
- To provide you with important notices about the Platform, including changes to our Terms or this Policy
- To send transactional communications (transaction confirmations, security alerts, account notifications)

## 5. HOW WE SHARE YOUR INFORMATION

Via Easy Pay does not sell your personal information. We share your personal information only in the following circumstances and with the following categories of recipients:

### 5.1 Third-Party Service Providers

We share personal information with Third-Party Service Providers who perform services on our behalf or whose services are integrated with the Platform, including:

- **On/Off-Ramp Providers:** Licensed financial services providers that facilitate the conversion between Fiat Currency and Digital Assets. When you initiate an On/Off-Ramp transaction, your identity data and transaction data are shared with the applicable provider to facilitate the transaction and comply with their regulatory obligations.
- **Identity Verification Providers:** Third-party KYC service providers that verify your identity on our behalf in accordance with applicable AML/CTF laws.

- **Blockchain Infrastructure Providers:** Providers of bundler, paymaster, and smart account infrastructure that facilitate blockchain transactions. Transaction data (including wallet addresses and transaction parameters) is shared as necessary to process your transactions.
- **Analytics Providers:** Third-party analytics services that help us understand Platform usage and improve our Services. Analytics data is aggregated and does not identify individual users.
- **Cloud Infrastructure Providers:** Third-party hosting and cloud computing providers that store and process data on our behalf.

Each Third-Party Service Provider operates under its own terms of service, privacy policy, and regulatory framework. We encourage you to review the privacy practices of any Third-Party Service Provider before using their services through our Platform.

**5.2 Regulatory Authorities and Law Enforcement**

We may disclose your personal information to regulatory authorities, law enforcement agencies, courts, or other governmental bodies when:

- Required by applicable law, regulation, legal process, or governmental request;
- Required to comply with AML/CTF reporting obligations (including Suspicious Transaction Reports, Large Virtual Currency Transaction Reports, and sanctions-related reports to FINTRAC, FinCEN, or other applicable authorities);
- We believe disclosure is necessary to protect the rights, property, or safety of Via Easy Pay, our users, or the public;
- We believe disclosure is necessary to detect, prevent, or address fraud, security issues, or technical problems.

**Note:** Via Easy Pay may be prohibited by law from informing you of certain disclosures to regulatory authorities.

**5.3 Corporate Affiliates**

We may share personal information between Dealing Media Inc. and Via Easy Pay Inc. for the purposes described in this Policy. Both entities operate under the Via Easy Pay brand and maintain equivalent data protection standards. See Section 7 for information about cross-border transfers.

### 5.4 Corporate Transactions

In the event of a merger, acquisition, reorganization, bankruptcy, asset sale, or similar corporate transaction, your personal information may be transferred as part of the transaction. We will provide notice of any such transfer and any choices you may have regarding your information.

### 5.5 With Your Consent

We may share your personal information with third parties when you have provided your explicit consent to such sharing.

### 5.6 Public Blockchain Data

**Important:** When you conduct transactions on a public blockchain network, certain transaction data — including your blockchain wallet address, transaction amounts, and transaction hashes — is recorded on the public blockchain and is inherently visible to anyone. This is a fundamental characteristic of public blockchain technology and is not within Via Easy Pay's control. Via Easy Pay cannot delete, modify, or restrict access to data recorded on public blockchains.

## 6. DATA RETENTION

### 6.1 Retention Periods

We retain your personal information only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable law. The following retention periods apply:

| Data Category | Retention Period | Legal Basis |
|---|---|---|
| Identity Data (KYC records) | 5 years from the date the account is closed or the last transaction, whichever is later | PCMLTFA regulatory requirement |
| Transaction Data | 5 years from the date of the transaction | PCMLTFA regulatory requirement |
| Biometric Data | Duration of active wallet plus 90 days, unless shorter period required by applicable law | See Section 8 |
| Device and Technical Data | 24 months from the date of collection | Legitimate business purposes |

| Data Category | Retention Period | Legal Basis |
|---|---|---|
| Usage Data | 24 months from the date of collection | Legitimate business purposes |
| Network and Location Data | 12 months from the date of collection | Legitimate business purposes |
| Communications Data | 36 months from the date of last communication | Customer support and legal purposes |
| AML/CTF Compliance Records | 5 years from the date of the record | PCMLTFA regulatory requirement |

### 6.2 Destruction

Upon expiration of the applicable retention period, personal information is securely destroyed using commercially appropriate methods, including:

- Electronic data: Secure deletion using industry-standard data sanitization methods that render the data unrecoverable
- Physical records (if any): Cross-cut shredding or incineration
- Third-Party Service Provider data: Destruction in accordance with our contractual data processing agreements

### 6.3 Exceptions

We may retain personal information beyond the stated retention periods where:

- Required by applicable law, regulation, or legal proceeding;
- Necessary for the establishment, exercise, or defense of legal claims;
- Required to comply with an ongoing regulatory investigation or audit;
- The information has been anonymized such that it can no longer identify any individual.

## 7. CROSS-BORDER DATA TRANSFERS

Via Easy Pay operates through two entities: Dealing Media Inc. (Ontario, Canada) and Via Easy Pay Inc. (Wyoming, United States). Your personal information may be transferred between these entities and processed in both Canada and the United States for the purposes described in this Policy.

### 7.1 Transfers Between Via Easy Pay Entities

Personal information collected by Dealing Media Inc. may be shared with Via Easy Pay Inc., and vice versa, for purposes including service delivery, regulatory compliance, security, and platform development. Both entities maintain equivalent data protection standards and are bound by this Policy.

### 7.2 Transfers to Third-Party Service Providers

Your personal information may be transferred to Third-Party Service Providers located in jurisdictions outside of Canada, including the United States and other countries. Such transfers are made for the purposes described in Section 5 and are subject to appropriate contractual safeguards.

### 7.3 Canadian Users

Under PIPEDA, Canadian users have the right to be informed about cross-border transfers of their personal information. By using the Platform, you consent to the transfer of your personal information to the United States and other jurisdictions as described in this Policy. You acknowledge that personal information transferred to other jurisdictions may be subject to the laws and disclosure requirements of those jurisdictions, including lawful access by government authorities, courts, and law enforcement.

### 7.4 Safeguards

Via Easy Pay implements appropriate technical and organizational safeguards to protect personal information during cross-border transfers, including:

- Contractual data protection clauses with Third-Party Service Providers
- Encryption of data in transit (TLS 1.3) and at rest (AES-256)
- Access controls limiting data access to authorized personnel
- Regular security assessments of Third-Party Service Providers

## 8. BIOMETRIC DATA — DEDICATED DISCLOSURE

**This section provides specific disclosures regarding the collection, use, retention, and destruction of Biometric Data as required by the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14, the Texas Capture or Use of Biometric Identifier Act ("CUBI"), Tex. Bus. & Com. Code §503.001, the Washington Biometric Identifier Law, RCW 19.375, and Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA").**

**For a standalone version of this disclosure, please see our Biometric Privacy Disclosure at viaeasypay.com/biometric-privacy.**

### 8.1 What Biometric Data We Collect

The Platform uses your device's native biometric authentication system (such as Apple Face ID, Apple Touch ID, Android Biometric API, or equivalent hardware-backed biometric systems) for wallet creation and transaction authorization. In connection with this functionality, Via Easy Pay collects and processes the following biometric identifiers:

- **Facial geometry data** — mathematical representations of facial features used for identity verification and authentication
- **Fingerprint data** — mathematical representations of fingerprint patterns used for authentication (where the user's device supports and the user elects to use fingerprint authentication)

**Important clarification:** Via Easy Pay utilizes your device's native biometric hardware and software (e.g., Apple's Secure Enclave, Android's TEE/StrongBox). In many cases, the raw biometric data (your actual facial scan or fingerprint image) never leaves your device's secure hardware module. Via Easy Pay receives a cryptographic attestation from your device confirming successful biometric verification, rather than the raw biometric template itself. However, to the extent that any biometric identifiers or biometric information (as defined by applicable law) are collected, transmitted, stored, or processed by Via Easy Pay or its service providers, this Section 8 applies in full.

### 8.2 Purpose of Collection

Via Easy Pay collects and uses Biometric Data solely for the following purposes:

- **Wallet Creation:** To verify your identity and bind your Self-Custodial Wallet to your person through device-native biometric authentication, ensuring that only you can access and control your wallet.
- **Transaction Authorization:** To authenticate your identity each time you initiate a transaction, ensuring that transactions can only be authorized by the verified wallet owner.

- **Security and Fraud Prevention:** To prevent unauthorized access to your wallet and to detect and prevent identity fraud.

Via Easy Pay does not use Biometric Data for any purpose other than those stated above.

**8.3 Retention Schedule**

Biometric Data is retained only for as long as necessary to fulfill the purposes for which it was collected:

- **Active accounts:** Biometric Data is retained for the duration of your active use of the Platform.
- **Account closure or inactivity:** Biometric Data is permanently destroyed within ninety (90) days following account closure, wallet deactivation, or your request for deletion, whichever occurs first.
- **Shorter period required by law:** If applicable law in your jurisdiction requires a shorter retention period, the shorter period applies.

In no event shall Biometric Data be retained for longer than three (3) years from the date of your last interaction with the Platform, regardless of account status.

**8.4 Destruction Protocol**

Upon expiration of the applicable retention period, or upon your request, Biometric Data is permanently destroyed using the following methods:

- Secure deletion from all production databases, backup systems, and redundant storage using industry-standard data sanitization methods (NIST SP 800-88 compliant) that render the data unrecoverable;
- Confirmation of destruction by automated verification processes;
- Notification to any Third-Party Service Providers that have received Biometric Data to destroy their copies in accordance with contractual obligations.

**8.5 No Sale or Disclosure**

**Via Easy Pay will not sell, lease, trade, or otherwise profit from your Biometric Data.** Via Easy Pay will not disclose your Biometric Data to any third party without your prior written consent, except:

- To Third-Party Service Providers who assist in providing the Services described in Section 8.2, and who are contractually bound to use Biometric Data solely for those purposes and to protect it in accordance with this Policy;
- As required by applicable law, regulation, legal process, or governmental request;
- As necessary to protect the rights, property, or safety of Via Easy Pay, its users, or the public.

### 8.6 Data Security

Biometric Data is protected by the following security measures:

- **Encryption at rest:** AES-256 encryption
- **Encryption in transit:** TLS 1.3
- **Access controls:** Biometric Data is accessible only to authorized personnel with a legitimate business need, subject to strict access controls and logging
- **Hardware security:** Where possible, biometric processing occurs within the secure hardware module of your device (e.g., Secure Enclave, TEE) and biometric templates do not leave the device
- **Segregation:** Biometric Data is stored separately from other personal information

### 8.7 Your Rights Regarding Biometric Data

You have the following rights with respect to your Biometric Data:

- **Right to information:** You have the right to be informed about the collection, use, retention, and destruction of your Biometric Data, which is provided through this Policy and our standalone Biometric Privacy Disclosure.
- **Right to consent:** Biometric Data is collected only with your prior informed consent, obtained through an affirmative consent mechanism before any biometric data is collected.
- **Right to withdraw consent:** You may withdraw your consent to the collection and use of Biometric Data at any time by contacting compliance@viaeasy.com. Withdrawal of consent may limit or prevent your ability to use certain features of the Platform that require biometric authentication.
- **Right to deletion:** You may request the deletion of your Biometric Data at any time by contacting compliance@viaeasy.com. We will process your deletion request within thirty (30) days.
- **Right to file a complaint:** If you believe your rights regarding Biometric Data have been violated, you may contact our Privacy Officer or file a complaint with the applicable regulatory authority.

### 8.8 Consent Mechanism

Before any Biometric Data is collected, Via Easy Pay obtains your informed, written consent through the following mechanism:

- A clear disclosure presented to you describing: (a) what Biometric Data will be collected; (b) the purpose of collection; (c) the retention period; and (d) the destruction protocol;
- An affirmative consent action (checking a consent box and clicking "I Consent") that must be completed before any biometric enrollment or authentication occurs;
- A record of your consent, including the date, time, and version of the disclosure presented, is maintained by Via Easy Pay.

## 9. SMS Communications

When you provide your mobile phone number to Via Easy Pay, or when a Via Easy Pay sender provides your mobile number to deliver a payment to you, you consent to receive transactional SMS messages from Via Easy Pay related to that payment, including delivery confirmations, claim links, and security notifications.

- Message Types: All SMS messages are transactional and tied to a specific payment event. Via Easy Pay does not send marketing or promotional SMS messages.
- Message Frequency: Message frequency is event-based and varies by sender activity. You will only receive SMS messages when a sender initiates a payment to your phone number or when a payment you initiated reaches a status milestone.
- Opt-In Mechanism: Via Easy Pay uses third-party / sender-initiated opt-in. Senders attest, when entering a recipient's phone number, that they have permission to contact that recipient. Recipients may opt out at any time by replying STOP.
- Opt-Out: Reply STOP to any Via Easy Pay SMS to immediately stop all future SMS messages from Via Easy Pay. Reply HELP for support information.
- Message and Data Rates: Standard message and data rates from your mobile carrier may apply. Via Easy Pay does not charge any fees for SMS messages.
- No Sale of Phone Numbers: Via Easy Pay does not sell, rent, share, or transfer phone numbers to third parties for marketing purposes. Phone numbers are used solely to deliver the transactional notifications described in this section.
- Carrier Disclaimer: Via Easy Pay is not liable for delayed or undelivered messages caused by carrier issues, device issues, or international routing.

## 9. COOKIES AND TRACKING TECHNOLOGIES

### 9.1 What Are Cookies

Cookies are small text files that are placed on your device when you visit a website. They are widely used to make websites work more efficiently and to provide information to website operators.

### 9.2 Categories of Cookies

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

**Strictly Necessary Cookies** — These cookies are essential for the Platform to function and cannot be disabled. They include cookies that maintain your session, enable security features, and facilitate core Platform functionality. These cookies do not require your consent.

**Functional Cookies** — These cookies enable enhanced functionality and personalization, such as remembering your preferences and settings. If you do not allow these cookies, some features of the Platform may not function properly.

**Analytical Cookies** — These cookies help us understand how users interact with the Platform by collecting usage data in an aggregated and anonymized form. We use this information to improve Platform performance and user experience.

**Marketing Cookies** — These cookies may be used to deliver content and advertisements that are relevant to your interests. As of the date of this Policy, Via Easy Pay does not use marketing cookies. If we introduce marketing cookies in the future, we will update this Policy and obtain your consent where required.

### 9.3 Consent

When you first visit the Platform, a cookie consent banner will be displayed allowing you to:

- Accept all cookies
- Reject non-essential cookies (accepting only strictly necessary cookies)
- Manage your cookie preferences by category

Your cookie preferences can be changed at any time through the Platform's cookie settings.

### 9.4 Third-Party Cookies

Some cookies may be placed by Third-Party Service Providers whose services are integrated with the Platform, such as analytics providers. These third parties have their own privacy policies governing the use of cookies and the processing of data collected through them.

### 9.5 Disabling Cookies

You can also control cookies through your browser settings. Most browsers allow you to block or delete cookies. Please note that blocking or deleting cookies may affect the functionality of the Platform.

For more information about cookies, including how to manage and delete them, visit www.allaboutcookies.org.

## 10. YOUR RIGHTS

### 10.1 Rights Under PIPEDA (Canadian Users)

If you are a resident of Canada, you have the following rights under PIPEDA:

- **Right of Access:** You have the right to request access to the personal information we hold about you. We will respond to your request within thirty (30) days of receipt, subject to limited exceptions permitted by PIPEDA.
- **Right of Correction:** You have the right to request that we correct any inaccurate or incomplete personal information we hold about you.
- **Right to Withdraw Consent:** You have the right to withdraw your consent to the collection, use, or disclosure of your personal information, subject to legal or contractual restrictions and reasonable notice. Withdrawal of consent may affect your ability to use the Platform.
- **Right to File a Complaint:** You have the right to file a complaint with the Office of the Privacy Commissioner of Canada regarding our handling of your personal information.

To exercise any of these rights, please contact our Privacy Officer at compliance@viaeasy.com. We may require you to verify your identity before processing your request.

### 10.2 Rights Under US State Privacy Laws

If you are a resident of a US state with applicable privacy legislation, you may have additional rights, including:

- **Right to Know / Access:** The right to know what personal information we collect and to request access to your personal information.

- **Right to Delete:** The right to request the deletion of your personal information, subject to exceptions.
- **Right to Correct:** The right to request correction of inaccurate personal information.
- **Right to Non-Discrimination:** The right not to be discriminated against for exercising your privacy rights.
- **Right to Opt Out of Sale:** Via Easy Pay does not sell personal information. However, if applicable law provides you with a right to opt out of the sale of personal information, you may exercise this right by contacting compliance@viaeasy.com.

**10.3 Exercising Your Rights**

To exercise any of your privacy rights, please contact our Privacy Officer at:

Email: compliance@viaeasy.com

We will respond to all verified requests within thirty (30) days of receipt. If we require additional time (up to an additional thirty (30) days), we will notify you of the extension and the reason for it.

We may require you to verify your identity before processing your request. We will not charge a fee for processing your request unless the request is manifestly unfounded, excessive, or repetitive.

**11. DATA SECURITY**

**11.1 Security Measures**

Via Easy Pay implements commercially reasonable technical and organizational security measures to protect your personal information from unauthorized access, disclosure, alteration, destruction, or loss. These measures include:

- **Encryption:** All data is encrypted in transit using TLS 1.3 and at rest using AES-256 encryption.
- **Access Controls:** Access to personal information is restricted to authorized personnel on a need-to-know basis, subject to role-based access controls, multi-factor authentication, and logging.
- **Infrastructure Security:** The Platform is hosted on secure cloud infrastructure with industry-standard security certifications.
- **Monitoring:** Continuous monitoring of systems and networks for unauthorized access and anomalous activity.

- **Employee Training:** Regular privacy and security awareness training for all personnel who handle personal information.
- **Vendor Assessment:** Security assessments of Third-Party Service Providers before engagement and on an ongoing basis.

### 11.2 Breach Notification

In the event of a data breach involving your personal information that creates a real risk of significant harm, Via Easy Pay will:

- Notify affected individuals as soon as feasible after the breach is discovered;
- Report the breach to the Office of the Privacy Commissioner of Canada (for breaches involving Canadian users' personal information) as required by PIPEDA's mandatory breach notification provisions;
- Report the breach to any other applicable regulatory authority as required by law;
- Maintain a record of all breaches of security safeguards, regardless of whether they meet the reporting threshold.

### 11.3 Limitations

While we take commercially reasonable steps to protect your personal information, no method of transmission over the internet or method of electronic storage is 100% secure. We cannot guarantee the absolute security of your personal information.

## 12. CHILDREN'S PRIVACY

The Platform and Services are not directed to, and not intended for use by, persons under the age of eighteen (18). Via Easy Pay does not knowingly collect personal information from persons under the age of eighteen (18). If we become aware that we have inadvertently collected personal information from a person under the age of eighteen (18), we will take commercially reasonable steps to delete such information as soon as practicable.

If you are a parent or guardian and believe that your child has provided personal information to Via Easy Pay, please contact our Privacy Officer at compliance@viaeasy.com.

## 13. DO NOT TRACK SIGNALS

Some web browsers transmit "Do Not Track" (DNT) signals to websites. Because there is no universally accepted standard for how to respond to DNT signals, the Platform does not currently respond to DNT signals. However, you can manage your cookie preferences as described in Section 9.

## 14. CHANGES TO THIS POLICY

Via Easy Pay reserves the right to update or modify this Policy at any time. For material changes, we will provide at least fourteen (14) days' advance notice before the revised Policy takes effect. Notice may be provided by:

- Posting the updated Policy on the Platform with a revised "Last Updated" date;
- Sending notification to the email address associated with your account;
- Displaying a prominent notice on the Platform.

Your continued use of the Platform after the effective date of the revised Policy constitutes your acceptance of the changes. We encourage you to review this Policy periodically to stay informed about our privacy practices.

## 15. CONTACT INFORMATION

If you have any questions about this Policy, wish to exercise your privacy rights, or have a privacy-related complaint, please contact:

**Privacy Officer** Via Easy Pay Email: compliance@viaeasy.com

**For Canadian Users:** Dealing Media Inc. O/A Via Easy 3898 Chesswood Drive, North York, Ontario M3J 2W6, Canada

**For United States and International Users:** Via Easy Pay Inc. 1309 Coffeen Avenue STE 1200, Sheridan, Wyoming 82801, USA

**Office of the Privacy Commissioner of Canada:** 30 Victoria Street, Gatineau, Quebec K1A 1H3 Toll-free: 1-800-282-1376 Website: www.priv.gc.ca

*Via Easy Pay is a payment technology infrastructure provider. Via Easy Pay is not a bank, authorized deposit-taking institution, broker-dealer, or investment advisor. Via Easy Pay does not hold deposits and is not insured by the FDIC, CDIC, CIPF, SIPC, or any similar deposit or investor protection scheme. Digital assets are volatile and may lose value. Confirmed blockchain transactions are irreversible. Unclaimed Via Easy Payment Links are automatically returned to the sender after the expiry period.*

*Dealing Media Inc. is registered as a Money Services Business with FINTRAC (Registration No. C100000282). Registration with FINTRAC does not indicate endorsement or licensing of this business by FINTRAC.*