Privacy Policy

Last Updated: February 24, 2026.

1. GENERAL PROVISIONS

This Privacy Policy (“Policy”) is issued by CARDFLY PAYMENTS LTD., a company incorporated under the laws of Canada with its registered address at 331 Somerset Street West, Ottawa, Ontario, K2P 0J8, Canada (“Cardfly”, “we”, “us”, or “our”). CARDFLY PAYMENTS LTD. operates the website www.advasend.com under the brand name “Advasend” (collectively, the “Platform”), and all Services made available through the Platform are provided by CARDFLY PAYMENTS LTD.

This Policy governs the collection, use, processing, storage, disclosure, and protection of Personal Data of individuals (“Users”, “you”, “your”) who access or use the Platform or the Services.

This Policy has been drafted in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA), the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), and other applicable Canadian laws and regulations, and where applicable, the EU General Data Protection Regulation (GDPR).

By accessing or using the Services, you acknowledge that you have read and understood this Policy. This Policy forms an integral part of the User Agreement, and any privacy-related inquiries may be directed to support@advasend.com.

2. CATEGORIES OF PERSONNAL DATA COLLECTED

CARDFLY PAYMENTS LTD. may collect, process, and retain the following categories of Personal Data:

2.1 Registration and Account Data

- Full name
- Residential address
- Date of birth
- Email address
- Telephone number
- Account credentials (username, password)
- Security preferences and authentication data

2.2 Identity Verification and Compliance (KYC/AML) Data

- Government-issued identification documents (e.g., passport, driver’s licence, national ID)
- Photographs, selfie images, and liveness verification data
- Proof of residential address
- Occupation and employer details

- Source of income and source of funds information
- Information regarding the purpose and intended nature of transactions
- Sanctions screening and Politically Exposed Person (PEP) screening results

2.3 Transaction Data

- Records of Transfers, funding transactions, withdrawals, and currency exchanges
- Payment method details (bank accounts, cards, wallets)
- Counterparty information (sender/recipient details)
- Transaction amounts, currencies, timestamps, and reference numbers

2.4 Technical and Device Data

- IP address
- Device identifiers and specifications
- Operating system and browser type
- Approximate geolocation (city-level)
- Session activity logs and security event data

2.5 Communication Data

- Emails and customer support correspondence
- Chat transcripts and call recordings (where applicable)
- Feedback, survey responses, and user engagement data

2.6 Data from Third Parties

- Information obtained from financial institutions and payment processors
- Identity verification and sanctions screening providers
- Fraud prevention databases
- Regulatory and law enforcement authorities, where applicable

3. LEGAL BASIS FOR PROCESSING

Cardfly processes Personal Data on one or more of the following legal grounds:

- **Performance of a Contract**: Processing is necessary to provide the Services, administer the Account, execute transactions, and fulfil obligations under the User Agreement.
- **Compliance with Legal Obligations**: Processing is required to comply with applicable laws and regulations, including but not limited to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), sanctions regulations, tax reporting requirements, and other statutory obligations.
- **Legitimate Interests**: Processing is necessary for Cardfly's legitimate business interests, including fraud prevention, risk management, security monitoring, service improvement, analytics, and internal administrative purposes, provided that such interests are not overridden by the User's rights and freedoms.

- **Consent:** Where required by applicable law, processing is based on the User's consent, including for marketing communications or certain types of optional data processing. Consent may be withdrawn at any time, subject to legal or contractual limitations.

Where Personal Data is required to comply with legal obligations or to perform a contract, failure to provide such data may result in inability to open an Account, complete identity verification, or access certain Services.

4. DATA SUBJECT RIGHTS

Subject to applicable law, Users shall enjoy the following rights in respect of their Personal Data:

- Right to be informed of the collection and use of Personal Data
- Right of access to obtain confirmation and a copy of the data held
- Right to rectification of inaccurate or incomplete data
- Right to erasure ("right to be forgotten"), unless retention is required by law (e.g., PCMLTFA recordkeeping)
- Right to restriction of processing under certain circumstances
- Right to data portability, in machine-readable format, where technically feasible
- Right to object to processing carried out on the basis of legitimate interests, including direct marketing
- Right to withdraw consent at any time

All rights requests shall be directed to: support@advasend.com.

5. DATA RETENTION

5.1. Cardfly retains Personal Data only for as long as necessary to fulfil the purposes set out in this Policy and to comply with applicable legal and regulatory obligations. In particular:

- Identity verification (KYC) and AML/CTF records, including identification documents and transaction records, are retained for a minimum of five (5) years following the closure of the Account, in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).
- Transactional records are retained for at least five (5) years from the date of the Transfer, or longer where required by law.
- Communication records, including customer support correspondence, may be retained for compliance, dispute resolution, and risk management purposes.

- Marketing data is retained until the User withdraws consent or unsubscribes from marketing communications.

5.2. Personal Data may be retained beyond the standard retention periods where required for the establishment, exercise, or defence of legal claims, ongoing regulatory investigations, fraud prevention, or compliance with legal obligations.

5.3. Upon expiration of the applicable retention period, Personal Data will be securely deleted, anonymised, or otherwise disposed of in accordance with applicable data protection requirements.

6. SECURITY MEASURES

6.1. Cardfly implements appropriate technical, organisational, and administrative safeguards designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

- Security measures include, without limitation:
- Encryption of Personal Data in transit and, where appropriate, at rest;
- Multi-factor authentication (MFA) and secure authentication protocols;
- Access controls restricting Personal Data to authorized personnel on a need-to-know basis;
- Continuous monitoring of systems for suspicious activity and security incidents;
- Regular security testing, vulnerability assessments, and internal audits;
- Employee training and confidentiality obligations;
- Secure data storage infrastructure and reputable third-party hosting providers.

6.2. Cardfly maintains internal policies and procedures to respond to suspected data breaches and security incidents in accordance with applicable legal requirements.

6.3. While Cardfly applies commercially reasonable security measures, no system can be guaranteed to be completely secure, and Users acknowledge that transmission of information over the internet involves inherent risks.

7. DISCLOSURE TO THIRD PARTIES

7.1. Cardfly does not sell, rent, or lease Personal Data. Personal Data may be disclosed where necessary to provide the Services, comply with legal or regulatory obligations, or protect Cardfly’s legitimate interests.

7.2. Personal Data may be shared with financial institutions and payment processors for transaction execution; identity verification, AML/CTF, and sanctions screening providers; technology, cloud hosting, and infrastructure service providers; professional advisors; and competent regulatory, supervisory, or law enforcement authorities where required by law or lawful request.

7.3. All third-party disclosures are made subject to appropriate contractual, confidentiality, and data protection safeguards designed to ensure compliance with applicable data protection laws.

8. INTERNATIONAL TRANSFERS

8.1. Personal Data may be processed, stored, or accessed outside of Canada where Cardfly's service providers, partners, or infrastructure are located in other jurisdictions.
8.2. Where Personal Data is transferred outside Canada, Cardfly takes reasonable steps to ensure that such data remains protected in accordance with applicable data protection laws. This may include the implementation of contractual safeguards, confidentiality obligations, and other appropriate measures designed to ensure an adequate level of protection.
8.3. Users acknowledge that Personal Data transferred to other jurisdictions may be subject to the laws of those jurisdictions and may be accessible to courts, law enforcement, and national security authorities in accordance with applicable law.

9. COOKIES AND TRACKING TECHNOLOGIES

9.1. The Platform uses cookies and similar tracking technologies (such as pixels and SDKs) to operate the Platform, enable core functionality (including login and security features), remember user preferences, analyse usage and performance, and (where permitted) deliver and measure marketing communications.
9.2. Cookies may be set by Cardfly ("first-party cookies") or by third-party service providers that support the Platform's functionality, analytics, or marketing. You can manage or disable cookies through your browser or device settings, and, where available, through cookie preference tools on the Platform; however, disabling certain cookies may affect the availability or functionality of the Services.
9.3. Where required by applicable law, Cardfly will obtain your consent before placing non-essential cookies and you may withdraw your consent at any time by adjusting your cookie settings.

10. ACCOUNT DELETION

10.1. Users may request closure of their Account after completing all pending transactions and satisfying any applicable verification or compliance requirements. Upon closure, access to the Services will be terminated.
10.2. Notwithstanding any deletion request, Cardfly is required to retain certain Personal Data, including identity verification (KYC) records and transactional data, for a minimum of five (5) years following account closure in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and other applicable legal obligations.
10.3. Personal Data may be retained beyond standard retention periods where necessary for compliance with regulatory requirements, the establishment, exercise, or defence of legal claims, fraud prevention, dispute resolution, or ongoing investigations. After expiration of applicable retention periods,

Personal Data will be securely deleted, anonymised, or otherwise disposed of in accordance with applicable data protection requirements.

11. AMENDMENTS

11.1. Cardfly may amend or update this Privacy Policy from time to time to reflect changes in legal requirements, operational practices, or regulatory obligations.

11.2. Updated versions will be published on the Platform with an updated “Last Updated” date. Continued use of the Services after publication of a revised Policy constitutes acknowledgment of the updated terms.

12. CONTACT INFORMATION

For all matters relating to this Privacy Policy or the processing of Personal Data, Users may contact:

Chief Technology Officer (CTO)
CARDFLY PAYMENTS LTD.
331 Somerset Street West
Ottawa, Ontario, K2P 0J8
Canada

Email: support@advasend.com