NectraPay Privacy Policy

Effective Date: April 1, 2026 | **Version:** 1.0 | TAMIMI DRAFT

About This Privacy Policy

NectraPay (trading as Nectra Payment Solutions FZE) is a regulated virtual asset payment processor operating under the supervision of the Virtual Assets Regulatory Authority (VARA) in the United Arab Emirates.

This Privacy Policy describes how we collect, use, store, share, and protect your personal data when you:

- Visit our website at www.nectrapay.com
- Register as a merchant on our Platform
- Use our payment processing services
- Interact with our customer support
- Engage with our APIs and technical integrations

This Policy applies to all users globally and should be read in conjunction with our Terms and Conditions, Cookie Policy, and Acceptable Use Policy.

---

1. Who We Are

Legal Entity: Nectra Payment Solutions FZE (To be changed)
Trade Name: NectraPay
Jurisdiction: United Arab Emirates (Dubai)
Regulatory Status: Licensed Virtual Asset Service Provider (VASP) under VARA
Registration Number: [To be inserted upon VARA license issuance]

Contact Information:

- **Data Protection Officer:** privacy@nectrapay.com
- **Compliance Officer:** compliance@nectrapay.com

- **Registered Address:** [Dubai Free Zone Address]
- **Website:** www.nectrapay.com

For the purposes of applicable data protection law (including GDPR, UK GDPR, and UAE PDPL), NectraPay acts as the **data controller** for personal data processed through our Platform.

---

2. Scope and Application

2.1 Who This Policy Covers

This Privacy Policy applies to:

- **Merchants** — businesses and individuals who register to accept payments via NectraPay
- **End Users / Customers** — individuals making payments to merchants through our Platform
- **Website Visitors** — anyone browsing www.nectrapay.com
- **Prospective Clients** — businesses inquiring about our services
- **Service Providers** — third parties providing services to NectraPay (subject to separate DPAs)

2.2 Children's Privacy

NectraPay does not knowingly collect personal data from individuals under the age of 18. Our services are intended exclusively for business use and adult consumers. If we become aware that we have inadvertently collected data from a minor, we will delete it promptly.

2.3 Jurisdictional Application

NectraPay operates globally and processes data in accordance with:

- UAE Personal Data Protection Law (Federal Decree-Law No. 45/2021)
- VARA Data Governance and Information Security Standards
- EU General Data Protection Regulation (GDPR) — for EEA residents
- UK GDPR and Data Protection Act 2018 — for UK residents
- Canada's PIPEDA and Quebec Law 25 — for Canadian residents
- Applicable local data protection laws where services are provided

Where multiple frameworks apply, we adhere to the **highest standard of protection**.

---

3. Personal Data We Collect

We collect personal data directly from you, automatically through your use of our Platform, and from third-party sources necessary for compliance and service delivery.

3.1 Merchant Data (Business Clients)

When you register as a merchant, we collect:

Identity and Contact Information

- Full legal name (individual) or business name (entity)
- Date of birth and nationality
- Government-issued ID (passport, national ID, or driver's license)
- Residential or business address
- Email address and phone number
- Beneficial ownership information (for corporate merchants)

Business and Financial Information

- Business registration documents (trade license, articles of incorporation)
- Tax identification number (TIN) or VAT registration
- Bank account details (IBAN, SWIFT/BIC, account holder name)
- Virtual asset wallet addresses (if applicable)
- Business description and website URL
- Trading volumes and transaction history
- Proof of address (utility bill, bank statement)

Compliance and Risk Data

- Source of funds and source of wealth documentation
- Sanctions screening results
- Adverse media checks
- PEP (Politically Exposed Person) status
- Ultimate Beneficial Owner (UBO) declarations

- Enhanced due diligence (EDD) documentation where required

Platform Usage Data

- Dashboard activity and login history
- API usage logs and integration data
- Transaction metadata (amounts, timestamps, currencies)
- Payout requests and settlement history
- Support tickets and communications

3.2 End User / Customer Data

When a customer makes a payment through a NectraPay-integrated merchant, we collect:

Transaction Data

- Payment amount and currency
- Transaction timestamp and status
- Payment method used (card, bank transfer, virtual asset)
- Order or invoice reference number
- Device fingerprint and IP address
- Merchant identifier

Identity Data (where required for compliance)

- Name as it appears on payment instrument
- Billing address
- Email address (for transaction receipts)
- Phone number (for payment verification)

Note: NectraPay processes end-user data on behalf of merchants. In these cases, NectraPay acts as a **data processor** and the merchant acts as the **data controller**. End users should refer to the merchant's privacy policy for details on how their data is used beyond payment processing.

3.3 Website Visitor Data

When you visit www.nectrapay.com, we collect:

- IP address and geolocation (country-level)
- Browser type, version, and language settings

- Device type and operating system
- Pages visited, time spent, and navigation paths
- Referral source (how you arrived at our site)
- Cookie and tracking data (see Cookie Policy for details)

3.4 Communications Data

When you contact us via email, chat, or phone, we collect:

- Name and contact details
- Content of communications
- Support ticket history
- Call recordings (with prior notice and consent)
- Attachments and documents shared

3.5 Data from Third-Party Sources

We obtain data from:

Source Type	Data Obtained	Purpose
Identity Verification Providers (e.g., Onfido, Sumsub)	ID document verification, liveness checks, biometric data	KYC compliance
Sanctions Screening Services (e.g., Chainalysis, Elliptic)	Sanctions lists, PEP lists, adverse media	AML/CFT compliance
Credit Reference Agencies	Business credit reports, director information	Risk assessment
Blockchain Analytics	On-chain transaction history, wallet risk scores	Virtual asset compliance
Payment Networks (e.g., Visa, Mastercard)	Card BIN data, issuer information	Payment routing and fraud prevention
Open Banking Providers	Bank account ownership verification	Payment authentication

---

4. How We Use Your Personal Data

We process personal data only where we have a lawful basis and legitimate purpose.

4.1 Legal Bases for Processing

Legal Basis	Description	Examples
Contractual Necessity	Processing required to perform our services under your merchant agreement	Account setup, payment processing, settlements
Legal Obligation	Required by UAE law, VARA regulations, or international AML/CFT standards	KYC/AML checks, transaction monitoring, regulatory reporting
Legitimate Interest	Necessary for our business operations, provided it does not override your privacy rights	Fraud prevention, platform security, service improvement
Consent	You have explicitly agreed to the processing	Marketing communications, optional analytics

4.2 Purposes of Data Processing

We use your personal data for the following purposes:

A. Service Delivery

- Creating and managing merchant accounts
- Processing payments and executing transactions
- Facilitating settlements and payouts to merchant bank accounts
- Providing customer support and resolving disputes
- Maintaining platform uptime and performance

Legal Basis: Contractual Necessity, Legitimate Interest

B. Compliance and Risk Management

- Conducting Know Your Customer (KYC) verification
- Performing Anti-Money Laundering (AML) checks

- Screening against sanctions lists (OFAC, UN, EU, UAE)
- Monitoring transactions for suspicious activity (KYT — Know Your Transaction)
- Filing Suspicious Activity Reports (SARs) with UAE Financial Intelligence Unit
- Complying with VARA data governance requirements
- Responding to lawful requests from regulators and law enforcement

Legal Basis: Legal Obligation, Legitimate Interest

C. Security and Fraud Prevention

- Detecting and preventing fraudulent transactions
- Identifying unusual account activity or credential compromise
- Implementing device fingerprinting and behavioral biometrics
- Protecting against DDoS attacks and platform abuse
- Conducting security audits and penetration testing

Legal Basis: Legitimate Interest, Legal Obligation

D. Analytics and Service Improvement

- Analysing platform usage patterns to improve UX
- Conducting A/B testing on new features (with consent)
- Identifying technical issues and performance bottlenecks
- Developing new products and services
- Generating aggregated, anonymised reports for business intelligence

Legal Basis: Legitimate Interest, Consent (for non-essential analytics)

E. Marketing and Communications

- Sending service updates, security alerts, and platform notifications (essential)
- Sharing product announcements and new features (essential)
- Sending promotional offers and marketing materials (consent-based only)
- Conducting customer satisfaction surveys (consent-based)

Legal Basis: Contractual Necessity (essential), Consent (marketing)

---

5. Data Sharing and Disclosure

NectraPay does not sell, rent, or trade your personal data. We share data only where necessary for service delivery, compliance, or with your explicit consent.

5.1 Categories of Recipients

Recipient Category	Purpose	Data Shared	Legal Safeguards
Payment Networks (Visa, Mastercard, bank networks)	Transaction processing and settlement	Transaction data, merchant identifiers	PCI-DSS compliance, contractual DPAs
KYC/AML Providers (Onfido, Sumsub, Chainalysis)	Identity verification and compliance checks	ID documents, biometric data, transaction history	GDPR-compliant DPAs, ISO 27001 certification
Banking Partners	Merchant settlements and fiat currency operations	Bank account details, transaction amounts	Banking secrecy agreements, regulatory supervision
Virtual Asset Custodians	Cryptocurrency custody and transfer	Wallet addresses, transaction records	SOC 2 Type II audits, insurance coverage
Cloud Infrastructure Providers (AWS, Google Cloud)	Platform hosting and data storage	Encrypted data at rest and in transit	EU/US Data Privacy Framework, Standard Contractual Clauses
Customer Support Tools (Intercom, Zendesk)	Providing merchant and customer support	Name, email, support ticket content	GDPR-compliant DPAs, data minimisation
Regulatory Authorities (VARA, UAE FIU,	Compliance with legal obligations	All data relevant to	Legal obligation,

Recipient Category	Purpose	Data Shared	Legal Safeguards
international regulators)		regulatory request	official requests only
Law Enforcement	Responding to valid legal process (court orders, subpoenas)	Data specified in legal request	Legal obligation, lawful basis verified

5.2 International Data Transfers

NectraPay operates globally and may transfer data outside the UAE to jurisdictions including:

- European Union / EEA (for cloud hosting and analytics)
- United States (for technology providers and payment networks)
- Singapore (for regional data processing)

Where data is transferred to countries without an adequacy decision from UAE authorities, we implement appropriate safeguards:

- **Standard Contractual Clauses (SCCs)** approved by the European Commission
- **Data Processing Agreements (DPAs)** with all third-party processors
- **Certification under EU-US Data Privacy Framework** (where applicable)
- **Binding Corporate Rules** for intra-group transfers

You may request a copy of the transfer safeguards in place by contacting privacy@nectrapay.com.

5.3 Business Transfers

In the event of a merger, acquisition, or sale of assets, your personal data may be transferred to the successor entity. We will notify affected users in advance and provide options to object or delete data where legally permissible.

---

6. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes outlined in this Policy, unless a longer retention period is required by law.

6.1 Retention Periods by Data Category

Data Type	Retention Period	Legal Basis
Active Merchant Accounts	Duration of contract + 7 years after closure	VARA regulatory requirement
KYC/AML Documentation	7 years from account closure or last transaction	UAE AML law, VARA requirements
Transaction Records	7 years from transaction date	Financial record-keeping obligations
Inactive Accounts (no activity for 24 months)	Account data archived after 2 years, deleted after 7 years	Data minimisation principle
Rejected Merchant Applications	1 year from rejection	Fraud prevention, regulatory queries
Website Visitor Data	13 months (analytics cookies)	Consent-based, see Cookie Policy
Support Communications	3 years from ticket closure	Customer service quality, dispute resolution
Security Logs (login, API access)	90 days (active monitoring) + 2 years (archived)	Security incident investigation

6.2 Deletion After Retention Period

Upon expiry of the retention period, personal data is:

1. **Permanently deleted** from active systems
2. **Anonymised** where required for statistical purposes
3. **Archived securely** if subject to ongoing legal hold or regulatory investigation

You may request early deletion of your data by submitting a request to privacy@nectrapay.com, subject to our legal obligations to retain certain records.

7. Data Security

NectraPay implements industry-leading technical and organisational measures to protect personal data against unauthorised access, loss, or misuse.

7.1 Technical Security Measures

- **Encryption:** All data is encrypted in transit (TLS 1.3) and at rest (AES-256)
- **Access Controls:** Role-based access control (RBAC) with multi-factor authentication (MFA)
- **Network Security:** Firewalls, intrusion detection systems (IDS), DDoS protection
- **Secure Development:** Regular code reviews, penetration testing, vulnerability scanning
- **API Security:** OAuth 2.0 authentication, rate limiting, request signing
- **Data Segregation:** Logical separation of merchant data; no cross-merchant data access
- **Backup and Recovery:** Daily encrypted backups with geographically distributed redundancy

7.2 Organisational Security Measures

- **Employee Training:** Mandatory annual data protection and security awareness training
- **Background Checks:** Pre-employment screening for all staff with data access
- **Confidentiality Agreements:** All employees and contractors sign NDAs
- **Incident Response Plan:** 24/7 Security Operations Centre (SOC) with defined breach procedures
- **Third-Party Audits:** Annual ISO 27001 and SOC 2 Type II audits
- **Data Protection Impact Assessments (DPIAs):** Conducted for high-risk processing activities

7.3 Data Breach Notification

In the event of a data breach that poses a risk to your rights and freedoms, NectraPay will:

1. Notify the relevant supervisory authority within **72 hours** of discovery (GDPR/PDPL requirement)
2. Notify affected individuals **without undue delay** if high risk exists
3. Provide details of the breach, data affected, and remedial actions taken
4. Offer support measures (e.g., credit monitoring, password reset assistance)

Notifications will be sent to your registered email address and posted on www.nectrapay.com/security-notice.

---

8. Your Data Protection Rights

You have the following rights regarding your personal data, subject to applicable law and regulatory obligations:

8.1 Right of Access

Request confirmation of whether we process your data and receive a copy of your data in a structured format.

How to exercise: Submit a Data Subject Access Request (DSAR) to privacy@nectrapay.com
Response time: Within 30 days (extendable to 60 days for complex requests)

8.2 Right to Rectification

Request correction of inaccurate or incomplete data.

How to exercise: Log in to your merchant dashboard and update your profile, or contact privacy@nectrapay.com
Response time: Within 30 days

8.3 Right to Erasure ("Right to be Forgotten")

Request deletion of your data where:

- Data is no longer necessary for its original purpose
- You withdraw consent (where processing is based on consent)
- You object to processing and no overriding legitimate interest exists

- Data has been unlawfully processed

Limitation: This right does not apply where we are required to retain data by law (e.g., 7-year AML record-keeping requirement).

How to exercise: Submit a deletion request to privacy@nectrapay.com
Response time: Within 30 days

8.4 Right to Restriction of Processing

Request that we temporarily suspend processing your data where:

- You contest the accuracy of the data
- Processing is unlawful but you oppose deletion
- We no longer need the data but you need it for legal claims
- You have objected to processing pending verification of overriding grounds

How to exercise: Contact privacy@nectrapay.com
Response time: Within 30 days

8.5 Right to Data Portability

Receive your data in a machine-readable format (e.g., CSV, JSON) and transmit it to another service provider.

How to exercise: Request a data export via your merchant dashboard or email privacy@nectrapay.com
Response time: Within 30 days

8.6 Right to Object

Object to processing based on legitimate interest, including profiling for marketing purposes.

How to exercise: Opt out of marketing via the unsubscribe link in emails or contact privacy@nectrapay.com
Response time: Immediate for marketing; 30 days for other objections

8.7 Right to Withdraw Consent

Where processing is based on consent (e.g., marketing, optional analytics), you may withdraw consent at any time.

How to exercise: Update preferences in your account settings or contact privacy@nectrapay.com
Effect: Withdrawal does not affect the lawfulness of processing prior to withdrawal

8.8 Right to Lodge a Complaint

You have the right to lodge a complaint with a supervisory authority if you believe we have violated data protection law.

Relevant Authorities:

- **UAE:** UAE Data Office (dataoffice@tdra.gov.ae)
- **EU/EEA:** Your national data protection authority (list at edpb.europa.eu)
- **UK:** Information Commissioner's Office (ico.org.uk)
- **Canada:** Office of the Privacy Commissioner of Canada (priv.gc.ca)

---

9. Cookies and Tracking Technologies

NectraPay uses cookies and similar technologies (web beacons, pixels, local storage) to operate our Platform and analyse usage. For full details on:

- Types of cookies deployed
- Purposes and legal bases
- Third-party cookies
- How to manage cookie preferences

Please refer to our **Cookie Policy** at www.nectrapay.com/legal/cookies.

---

10. Marketing Communications

10.1 Types of Communications

Essential Communications (No Opt-Out):

- Account activation and verification emails
- Transaction confirmations and settlement notifications

- Security alerts and suspicious activity warnings
- Service updates affecting your account
- Regulatory or legal notices

Marketing Communications (Consent-Based):

- Product announcements and new features
- Educational content (webinars, guides, case studies)
- Promotional offers and discounts
- Customer surveys and feedback requests

10.2 Consent and Opt-Out

Marketing communications are sent only with your explicit consent. You may opt out at any time by:

- Clicking "Unsubscribe" in any marketing email
- Updating your preferences in your merchant dashboard under Settings → Notifications
- Emailing privacy@nectrapay.com with "Unsubscribe" in the subject line

Effect of Opt-Out: You will stop receiving marketing communications within **48 hours**, but will continue to receive essential service communications.

---

11. Third-Party Links and Services

Our Platform may contain links to third-party websites, plugins, or services (e.g., merchant websites, social media platforms). NectraPay is not responsible for the privacy practices of these third parties.

We recommend you review the privacy policies of any third-party service before providing personal data.

Examples of Third-Party Integrations:

- Merchant checkout pages (merchant is data controller)
- Payment method providers (card networks, banks)
- Analytics tools (Google Analytics, Hotjar) — governed by our Cookie Policy

12. Merchant-Specific Obligations

12.1 Merchants as Data Controllers

When you integrate NectraPay to accept payments, **you remain the data controller** for your customers' personal data. You are responsible for:

- Providing your customers with a privacy notice explaining data collection and use
- Obtaining necessary consents for payment processing and data sharing
- Complying with data protection laws applicable to your business
- Ensuring your customers understand that NectraPay processes payment data on your behalf

12.2 Data Processing Agreement (DPA)

A Data Processing Agreement is incorporated into your merchant agreement, specifying:

- The scope and purpose of data processing
- NectraPay's obligations as a data processor
- Your obligations as data controller
- Data security and confidentiality requirements
- Sub-processor arrangements
- Data breach notification procedures
- Assistance with Data Subject Access Requests (DSARs)

You may request a standalone copy of the DPA by contacting legal@nectrapay.com.

12.3 Sub-Processors

NectraPay engages sub-processors to deliver payment services (e.g., KYC providers, banking partners, cloud infrastructure). A current list of sub-processors is available at www.nectrapay.com/legal/sub-processors.

Merchants will be notified **30 days in advance** of any changes to sub-processors, with the right to object.

13. Automated Decision-Making and Profiling

13.1 Fraud Detection and Risk Scoring

NectraPay uses automated systems to assess transaction risk and detect fraudulent activity. This includes:

- Real-time transaction risk scoring
- Device fingerprinting and behavioral analysis
- Machine learning models to identify suspicious patterns

Impact: High-risk transactions may be automatically flagged for manual review or declined to protect merchants and customers.

Your Rights: You have the right to request human review of an automated decision and to challenge the outcome. Contact compliance@nectrapay.com to exercise this right.

13.2 Credit and Merchant Underwriting

During merchant onboarding, we use automated systems to assess business risk and determine eligibility for services. This includes:

- Credit scoring based on business financials
- Industry risk classification
- Transaction volume projections

Impact: Applications may be automatically approved, referred for manual review, or declined based on risk thresholds.

Your Rights: You may request an explanation of the decision and human review by contacting compliance@nectrapay.com.

13.3 No Profiling for Marketing

NectraPay does **not** use automated profiling to deliver targeted advertising or personalised marketing. Marketing communications are based on general merchant segments (e.g., industry type, company size) and require explicit consent.

---

14. VARA-Specific Compliance

As a VARA-regulated Virtual Asset Service Provider, NectraPay adheres to the following data governance standards:

14.1 Data Governance Framework

- Designated Data Protection Officer (DPO) with VARA reporting line
- Board-level oversight of data protection and privacy risks
- Quarterly data governance audits and risk assessments
- Annual third-party audit of data protection controls

14.2 Data Localisation

VARA requires certain categories of data to be stored within the UAE or in VARA-approved jurisdictions. NectraPay maintains:

- **Primary data centre:** Dubai, UAE (AWS Middle East region)
- **Backup data centre:** EU (Ireland) — approved for redundancy
- **Disaster recovery:** Singapore (approved for business continuity)

14.3 Regulatory Reporting

NectraPay files the following reports with VARA:

- **Annual Data Processing Register** — comprehensive record of all data processing activities
- **Data Breach Notifications** — within 72 hours of discovery
- **Compliance Audits** — annual submission of ISO 27001 and SOC 2 reports
- **Data Transfer Impact Assessments** — for any new international data transfers

14.4 Transaction Monitoring and Reporting

In accordance with UAE AML law and VARA requirements, NectraPay:

- Monitors all transactions for suspicious activity using automated KYT systems
- Files Suspicious Transaction Reports (STRs) with the UAE Financial Intelligence Unit (FIU)
- Retains transaction data for 7 years for regulatory inspection
- Cooperates with VARA audits and information requests

Privacy Note: Transaction monitoring is conducted based on legal obligation and does not require consent. However, we implement data minimisation principles and restrict access to authorised compliance personnel only.

---

15. Changes to This Privacy Policy

NectraPay may update this Privacy Policy from time to time to reflect changes in:

- Our services and business practices
- Legal or regulatory requirements
- Technology and security standards

15.1 Notification of Changes

When we make material changes to this Policy:

1. The "Effective Date" at the top of this document will be updated
2. A prominent notice will be displayed on the Platform for **30 days**
3. Registered merchants will receive an email notification to their registered address
4. Where required by law, we will seek fresh consent for new processing activities

Your Continued Use: By continuing to use NectraPay services after the effective date of changes, you accept the updated Privacy Policy.

15.2 Version History

You may request previous versions of this Privacy Policy by emailing legal@nectrapay.com.

---

16. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

Data Protection Officer

Email: privacy@nectrapay.com
Response Time: Within 5 business days for general inquiries; within 30 days for formal data subject requests

Compliance Team

Email: compliance@nectrapay.com
Phone: [To be inserted]
Address: [Dubai Free Zone Address]

Legal Department

Email: legal@nectrapay.com
For: Contract inquiries, DPA requests, legal notices

Merchant Support

Email: support@nectrapay.com
Portal: https://merchant.nectrapay.com/support
Live Chat: Available Mon-Fri, 9am-6pm GST

---

17. Governing Law and Dispute Resolution

This Privacy Policy is governed by the laws of the **United Arab Emirates** and the regulatory framework established by **VARA**.

Any disputes arising from this Policy shall be resolved through:

1. Good faith negotiation between the parties
2. Mediation or arbitration in Dubai, UAE (if negotiation fails)
3. Jurisdiction of the Dubai International Financial Centre (DIFC) Courts (for DIFC-registered entities)

This does not affect your right to lodge a complaint with a data protection supervisory authority in your jurisdiction.

Appendix: Glossary of Terms

Term	Definition
Data Controller	The entity that determines the purposes and means of processing personal data
Data Processor	The entity that processes personal data on behalf of the data controller
DSAR	Data Subject Access Request — a formal request to access personal data
DPA	Data Processing Agreement — a contract governing processor obligations
GDPR	General Data Protection Regulation (EU Regulation 2016/679)
KYC	Know Your Customer — identity verification and due diligence process
KYT	Know Your Transaction — real-time transaction monitoring for AML compliance
PDPL	Personal Data Protection Law (UAE Federal Decree-Law No. 45/2021)
PII	Personally Identifiable Information
VASP	Virtual Asset Service Provider (regulated by VARA)
VARA	Virtual Assets Regulatory Authority (Dubai, UAE)

NectraPay is committed to protecting your privacy and ensuring compliance with the highest data protection standards globally.

Last Reviewed: April 2026
Next Scheduled Review: April 2027

Tags: #nectrapay #privacy-policy #legal #compliance #vara #gdpr #pdpl #data-protection