PRIVACY POLICY

1. IMPORTANT INFORMATION AND SCOPE OF THIS PRIVACY POLICY

TRANSACCT NEO – FZCO ("Company", "we", "our", or "us") recognises the importance of protecting personal data and is committed to ensuring that personal information is processed in accordance with applicable data protection legislation, including UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data ("UAE PDPL"), its implementing regulations, and internationally recognised privacy standards applicable to payment infrastructure providers.

This Privacy Policy explains how we collect, use, disclose, transfer, store and otherwise process personal data when individuals:

- access or use our website;
- interact with our payment processing infrastructure;
- use our platforms and related technical services (together, the "Services");
- communicate with us in connection with business relationships or transactions.

This Privacy Policy does not apply to third-party services, merchant environments, acquiring institutions, issuing banks, payment method providers or other external platforms integrated with our Services but operating independently from the Company.

Our website located at https://transacctneo.com (the "Site") may contain links to third-party websites. These websites operate independently and maintain their own privacy policies. We are not responsible for their content, policies or processing practices.

---

2. WHO WE ARE AND OUR ROLE IN DATA PROCESSING

TRANSACCT NEO – FZCO FZCO is a payment infrastructure and technology service provider established in Dubai Silicon Oasis under the regulatory framework of Dubai Integrated Economic Zones Authority (DIEZ).

Depending on the nature of a transaction and contractual arrangements with payment ecosystem participants, the Company may act either as:

- a data controller, where we independently determine the purposes and means of processing personal data; or

- a data processor, where personal data is processed strictly on behalf of merchants, payment service providers, acquiring institutions, financial institutions or other regulated entities.

Our role is determined by the structure of the transaction and the applicable contractual framework.

---

3. DATA PROTECTION PRINCIPLES

We process personal data in accordance with the following principles:

- lawfulness, fairness and transparency;
- purpose limitation;
- proportionality and data minimisation;
- accuracy;
- storage limitation;
- confidentiality and integrity;
- accountability.

Appropriate organisational and technical safeguards are applied regardless of where personal data is processed.

---

4. PERSONAL DATA WE COLLECT

Personal data means any information relating to an identified or identifiable individual. Anonymous information that cannot reasonably be linked to an individual is not considered personal data.

We collect personal data through direct interaction, automated technologies, merchants, payment participants and authorised third-party service providers.

---

5. INFORMATION COLLECTED THROUGH OUR WEBSITE

When you access or interact with our Site, we may collect the following categories of personal data.

5.1 Information provided directly by you

This may include:

- full name;
- email address;
- telephone number;
- company affiliation;
- website address;
- any information submitted through contact forms or correspondence.

5.2 Information collected automatically

We may automatically collect technical data including:

- IP address;
- browser type and version;
- operating system;
- device identifiers;
- geographic region of access;
- referral source;
- pages visited;
- duration of sessions;
- navigation behaviour across the Site.

This information may be collected using cookies, server logs, analytics tools and similar tracking technologies.

---

6. INFORMATION COLLECTED THROUGH OUR SERVICES

Where you interact with our payment processing infrastructure, we may collect the following categories of personal data.

6.1 Information provided by users or merchants

When registering for or using the Services:

- name and surname;
- email address;
- contact details;
- company details;
- account credentials;
- additional information required under applicable regulatory requirements.

6.2 Transaction-related personal data

Where you act as a payer, beneficiary or authorised representative of a merchant:

- billing address;
- delivery address;
- transaction amount;
- transaction date;
- transaction reference numbers;
- merchant identifiers;
- payment instrument metadata;
- masked card identifiers;
- bank account information where required for processing.

6.3 Compliance verification data

Where required under AML/CFT legislation or payment scheme rules:

- identity verification information;
- sanctions screening results;
- politically exposed person (PEP) indicators;
- fraud risk indicators;
- publicly available registry data;
- credit reference or fraud prevention datasets where permitted by law.

6.4 Technical and security information

To maintain infrastructure security and prevent misuse of Services:

- device fingerprinting data;
- firewall logs;
- behavioural transaction signals;
- session metadata;
- IP intelligence indicators.

6.5 Marketing-related information

Where permitted under applicable law, we may collect identity and contact information from publicly available professional directories or authorised commercial sources.

---

7. LEGAL BASIS FOR PROCESSING PERSONAL DATA

We process personal data on one or more of the following lawful bases:

- performance of contractual obligations;
- compliance with legal and regulatory obligations;
- protection of public interest;
- fraud prevention and security monitoring;
- legitimate operational interests of the Company;
- consent, where required under applicable legislation.

---

8. PURPOSES FOR WHICH WE PROCESS PERSONAL DATA

We process personal data only where necessary for legitimate operational purposes.

These purposes include:

8.1 Provision of Services

To:

- enable access to our infrastructure;
- administer accounts;
- maintain service continuity;
- support transaction execution;
- provide technical support.

8.2 Transaction processing

To:

- route payment instructions;
- communicate with payment ecosystem participants;
- enable settlement workflows;

- provide customer support related to transactions.

8.3 Regulatory compliance

To comply with:

- AML legislation;
- counter-terrorism financing regulations;
- sanctions obligations;
- payment scheme requirements;
- supervisory authority instructions.

8.4 Fraud prevention and infrastructure protection

To:

- detect suspicious activity;
- prevent unauthorised access;
- investigate misuse of Services;
- protect merchants and users;
- maintain platform integrity.

8.5 Customer communication

To:

- respond to enquiries;
- provide service notifications;
- deliver technical alerts;
- communicate policy updates.

8.6 Dispute resolution and enforcement of contractual rights

To:

- investigate complaints;
- resolve disputes;

- recover outstanding amounts;
- enforce contractual terms.

8.7 Service analytics and improvement

To:

- improve infrastructure performance;
- analyse platform usage;
- optimise user experience;
- develop new products and services.

8.8 Marketing communications

Where permitted by applicable law:

- newsletters;
- product updates;
- service announcements;
- promotional materials.

Recipients may opt out at any time.

---

9. AUTOMATED DECISION-MAKING

Certain processing activities may involve automated decision-making technologies designed to:

- detect fraud patterns;
- assess transaction risks;
- ensure compliance with regulatory requirements;
- prevent prohibited or restricted transactions.

Where required by law, individuals may request manual review of automated decisions affecting them.

---

10. DISCLOSURE OF PERSONAL DATA

We may disclose personal data to carefully selected third parties where necessary.

10.1 Payment ecosystem participants

Including:

- acquiring institutions;
- issuing banks;
- card schemes;
- payment method providers;
- settlement partners.

Only information necessary to execute transactions is shared.

10.2 Compliance and verification providers

Including:

- identity verification providers;
- AML monitoring platforms;
- sanctions screening vendors;
- fraud prevention service providers.

10.3 Technical infrastructure providers

Including providers supporting:

- hosting services;
- cybersecurity monitoring;
- analytics platforms;
- communication systems;
- IT infrastructure maintenance.

All such providers operate under contractual confidentiality obligations.

10.4 Payment scheme operators

Where transactions involve card-based payment instruments, personal data may be processed in accordance with the operating rules of international card schemes.

10.5 Corporate restructuring scenarios

Personal data may be disclosed in connection with:

- mergers;
- acquisitions;
- financing arrangements;
- asset transfers;
- corporate reorganisations.

10.6 Legal and regulatory disclosure obligations

We may disclose personal data where required:

- under applicable law;
- by regulatory authorities;
- by payment system operators;
- by courts or law enforcement agencies;
- to protect legal rights or prevent harm.

---

11. AML AND SANCTIONS SCREENING

Where required by applicable legislation and payment scheme rules, personal data may be processed through authorised compliance providers in order to:

- verify identity;
- perform sanctions screening;
- assess transaction risk;
- detect suspicious activity;
- prevent financial crime.

---

12. INTERNATIONAL TRANSFER OF PERSONAL DATA

Due to the global nature of payment processing infrastructure, personal data may be transferred outside the United Arab Emirates.

Where such transfers occur, the Company implements safeguards consistent with UAE PDPL requirements, including:

- transfers to jurisdictions providing adequate protection;
- contractual safeguards with service providers;
- organisational and technical protection measures;
- compliance with applicable regulatory frameworks governing payment infrastructure providers.

---

13. DATA SECURITY

We implement appropriate technical and organisational safeguards designed to protect personal data against:

- unauthorised access;
- accidental loss;
- unlawful disclosure;
- alteration or destruction.

Security measures include:

- encrypted transmission channels;
- firewall protection;
- restricted access permissions;
- monitoring infrastructure;
- internal confidentiality obligations.

Where required by law, affected individuals and regulators will be notified of personal data breaches.

---

14. DATA RETENTION

Personal data is retained only for as long as necessary to:

- provide Services;
- comply with regulatory obligations;
- resolve disputes;
- maintain accounting records;

- enforce contractual rights.

Retention periods depend on:

- transaction lifecycle;
- AML compliance requirements;
- statutory obligations;
- operational necessity;
- litigation exposure.

Where appropriate, personal data may be anonymised for statistical purposes.

---

15. COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies to:

- maintain session functionality;
- analyse website usage;
- improve platform performance;
- support security monitoring.

Users may manage cookie preferences through browser settings.

---

16. DATA ACCURACY

We take reasonable steps to ensure that personal data remains accurate and up to date.

Users are encouraged to notify us of any changes to their personal information.

---

17. YOUR RIGHTS

Subject to applicable legislation, individuals may have the right to:

- request access to personal data;
- request correction of inaccurate information;
- request deletion of personal data;
- request restriction of processing;
- object to processing;
- request portability of personal data;

- withdraw consent where applicable;
- request manual review of automated decisions.

Certain rights may be limited where processing is required by law or regulatory obligations applicable to payment service providers.

---

18. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy periodically to reflect:

- regulatory developments;
- infrastructure updates;
- service changes;
- security requirements.

Updated versions will be published on our website.

---

19. CONTACT DETAILS

Requests relating to personal data processing or the exercise of privacy rights may be submitted through the contact details available on our website:

https://www.transacctneo.com