UNIVERSAL PAYMENT NETWORK LIMITED

PRIVACY POLICY

Document Version: 1.0

Date of Issue: July, 2026

Table of Contents

1. Introduction

At **Unipaynet**, we are committed to protecting your privacy and safeguarding the personal information you entrust to us. We recognize the importance of your personal data and are dedicated to processing it in a lawful, fair, transparent, and secure manner.

This Privacy Notice explains how Unipaynet collects, uses, stores, shares, and protects your personal data whenever you access or use our products and services. It also outlines your rights regarding your personal information and our responsibilities in handling it.

This Privacy Notice applies whenever you:

- Visit the **Unipaynet website**.
- Access or use the **Unipaynet Mobile Application**.
- Use any Unipaynet services through our website, mobile application, or USSD platform.
- Contact or communicate with us through our customer support channels, including email, telephone, social media, live chat, or any other official communication platform.
- Register for, apply for, or use any Unipaynet products or services.

This Privacy Notice is designed to help you understand:

What You Will Learn	Description
Who We Are	Information about Unipaynet and the entity responsible for processing your personal data.
What Information We Collect	The categories of personal data we collect and the sources from which it is obtained.
Why We Process Your Information	The purposes for collecting and using your personal data and the legal grounds for doing so.
How We Protect Your Information	The technical, organizational, and administrative measures we implement to safeguard your personal data.
How We Share Your Information	The circumstances under which your personal data may be shared with trusted third parties or regulatory authorities.
Your Privacy Rights	The rights available to you regarding your personal data and how you can exercise them.
How to Contact Us	How to contact Unipaynet or the relevant data protection authority if you have any questions, concerns, or complaints regarding the processing of your personal data.

We encourage you to read this Privacy Notice carefully before using our products and services. By accessing or using our website, mobile application, or any of our services, you acknowledge that you have read and understood how we collect, use, and protect your personal information in accordance with this Privacy Notice.

2. About Unipaynet

Unipaynet Group comprises a number of affiliated entities that operate together to provide digital financial services, payment solutions, and related products. Depending on the nature of the product or service you access, the specific Unipaynet entity responsible for delivering that product or service will be identified to you at the time of registration, onboarding, or service engagement.

The Unipaynet entity providing your selected product or service will act as the **Data Controller** for your personal data. As the Data Controller, that entity is responsible for determining the purposes and means by which your personal information is collected, processed, stored, and protected, in accordance with applicable data protection and privacy laws.

Unipaynet is committed to ensuring that all processing of personal data is conducted lawfully, fairly, transparently, and in a manner that respects your privacy rights.

3. Scope of This Privacy Notice

This Privacy Notice explains how Unipaynet collects, uses, stores, shares, and protects your personal data when you access or use our products, services, and digital platforms.

This Privacy Notice applies to personal information collected through the following platforms and services:

- The Unipaynet website: **www.unipaynet.com**
- The Unipaynet mobile application
- Our USSD platform
- Any other digital channels, platforms, or services operated or provided by Unipaynet

In addition to information collected directly from you, Unipaynet may obtain personal data from other lawful sources, including trusted third-party service providers, regulatory authorities, financial institutions, payment networks, fraud prevention services, and other permitted sources where necessary to provide, secure, or improve our services.

Where additional personal information is required for a specific product, service, or legal obligation, we will provide you with an additional privacy notice or relevant disclosure before collecting and processing such information.

For the purposes of this Privacy Notice, **personal data** means any information relating to an identified or identifiable individual. An individual may be identified directly or indirectly through information such as an identifier, account details, device information, transaction records, or other personal characteristics.

Examples of personal data that Unipaynet may process include, but are not limited to:

- Your full name, identification details, and contact information.
- Your account information and customer profile details.
- Transaction details and payment information associated with your use of Unipaynet services.
- Your mobile number, email address, device information, and digital identifiers.
- Information required to verify your identity, comply with regulatory obligations, and prevent fraud or financial crime.

Unipaynet processes personal data only for legitimate business purposes, including providing services to customers, improving user experience, maintaining security, complying with legal and regulatory requirements, and protecting the rights and interests of our customers and the company.

If you have any questions, concerns, or requests regarding the processing of your personal data or the exercise of your privacy rights, you may contact our Data Protection Officer using the details below:

Data Protection Officer
Email: data@unipaynet.com

4. Personal Data We Collect About You

The personal data that Unipaynet collects and processes depends on the products, services, and features you access or use. We collect personal data from you directly, automatically through your interaction with our platforms, and from other lawful sources where necessary to provide our services, comply with regulatory obligations, manage risks, and protect our customers.
The categories of personal data we may collect include the following:

4.1 Information You Provide to Us ("Submitted Information")

We collect personal data that you voluntarily provide when you interact with Unipaynet, including when you:

Activity	Examples
Register for a Unipaynet account	Creating an account, providing registration details, and completing onboarding requirements
Open or manage an account	Updating account information, managing preferences, or accessing our services
Complete forms or applications	Providing information required for products, services, or account requests
Communicate with Unipaynet	Contacting customer support through email, telephone, social media, or the Unipaynet application
Participate in surveys, promotions, or customer research	Providing feedback, opinions, or responses
Engage with Unipaynet online	Participating in discussions, campaigns, or interactions through our digital platforms
Perform payment transactions	Sending money, receiving payments, topping up accounts, transferring funds, or exchanging electronic money

The personal data we collect may include:

Category	Personal Data Collected
Identity Information	Full name, date of birth, nationality, government-issued identification documents, and identity verification information
Contact Information	Residential address, telephone number, email address, and country of residence
Account Information	Username, Unipaynet Tag, account registration details, and customer profile information
Financial Information	Bank account details, payment card information, transaction details, beneficiary information, and payment records
Card Information	Details of registered payment cards, including card number, expiry date, and security verification details where applicable and permitted by law
Regulatory Information	Tax Identification Number (TIN), compliance information, and information required for regulatory reporting
Communication Records	Records of communications with Unipaynet, including customer support interactions, emails, messages, and telephone conversations

Identity Verification Data	Photographs, videos, and other biometric or verification information submitted during Know Your Customer (KYC) processes
Transaction Information	Details of recipients, beneficiaries, payment instructions, and information required to complete transactions
Additional Information	Any other information you provide to demonstrate eligibility for our products and services

We process this information where necessary to establish and perform our contractual relationship with you, comply with legal and regulatory obligations, protect our legitimate interests, or where you have provided consent.

4.2 Information Collected Through Your Use of Our Products and Services

When you use the Unipaynet mobile application, website, USSD platform, or other digital services, we may automatically collect technical, transactional, and usage information.

Category	Details of Information Collected
Device and Technical Information	Internet Protocol (IP) address, device type, operating system, browser type and version, mobile network information, unique device identifiers, application version, and security-related information
Account Access Information	Login details, authentication information, access records, and security logs
Website and Application Usage Information	Pages visited, features accessed, search activity, session duration, interaction history, technical errors, and performance information
Transaction Information	Transaction date and time, transaction amount, currencies used, exchange rates, sender and recipient details, beneficiary information, transaction location, payment method, device information, and related transaction messages
Digital Content Information	Information stored on your device where you provide permission, including contacts, photos, videos, or other content required to support specific services or features
Service Usage Information	Details of how you use Unipaynet services, including payment activities, transfers, foreign exchange transactions, and interactions with our platforms

We process this information based on our legitimate interests to operate, secure, maintain, improve, and personalize our services, enhance customer experience, prevent fraud, and ensure the reliability of our platforms.

4.3 Location Information

Where permitted by applicable laws and where you provide the required permissions, Unipaynet may collect and process location information obtained through technologies such as GPS, mobile networks, and IP address information.

Location data may be used for purposes including:

Purpose	Description

Fraud Prevention	Detecting suspicious activities, unusual transaction patterns, and potential unauthorized account access
Security Monitoring	Verifying transaction authenticity and protecting customers from financial crime
Service Enhancement	Improving the accuracy, security, and functionality of our services

For example, significant differences between your registered location, device location, and transaction activity may indicate potential fraud risks and may require additional verification before processing a transaction.

Where location processing requires consent under applicable law, you will be asked to provide permission before this information is collected. You may withdraw your consent at any time by adjusting location permissions through your device settings. However, disabling location access may affect the availability or functionality of certain Unipaynet features.

4.4 Information Obtained From Third Parties

To provide secure and reliable financial services, Unipaynet may receive personal data from authorized third parties, including:

Source	Examples of Information
Payment Service Providers and Financial Institutions	Transaction verification information, payment details, and settlement information
Identity Verification Providers	Identity verification results, document validation information, and fraud screening data
Regulatory and Government Authorities	Information required for compliance with legal and regulatory obligations
Business Partners and Service Providers	Information necessary to provide additional services, technical support, payment processing, analytics, or security services
Fraud Prevention and Risk Management Providers	Information used to detect, prevent, and investigate fraud, money laundering, and other financial crimes

Further details regarding how we share personal data with third parties are provided in the **"Disclosure and Sharing of Personal Information"** section of this Privacy Notice.

4.5 Information Obtained From Social Media Platforms

Where appropriate and permitted by law, Unipaynet may collect publicly available information from social media platforms or other online sources for purposes such as:

- Enhanced customer due diligence.
- Identity verification.
- Fraud prevention.
- Compliance with anti-money laundering (AML), counter-terrorist financing (CTF), and sanctions screening obligations.

We only collect and use publicly available information where there is a lawful basis for doing so and where such processing supports our legal, regulatory, or security obligations.

4.6 Information Obtained From Publicly Available Sources

Unipaynet may collect information from publicly available sources, including:

Source	Purpose
Public registers and official databases	Identity verification, regulatory compliance, and customer due diligence
Online directories and websites	Verification and risk assessment purposes
Media publications and publicly available records	Enhanced due diligence, fraud prevention, and reputational risk assessments

Such information may be used to support our obligations relating to customer verification, financial crime prevention, regulatory compliance, and service security.

Unipaynet is committed to collecting and processing personal data responsibly, transparently, and securely. We only collect information that is necessary, relevant, and proportionate for the purposes for which it is processed.

5. Legal Basis for Processing Your Personal Data

Unipaynet is committed to processing personal data in a lawful, fair, and transparent manner. We only collect and use your personal data where we have a valid legal basis to do so under applicable data protection and privacy laws.
Depending on the nature of the services provided, the purposes of processing, and our legal obligations, Unipaynet may rely on one or more of the following lawful bases:

Legal Basis	Explanation
Performance of a Contract (Contractual Necessity)	We process your personal data where it is necessary to establish, perform, or manage our contractual relationship with you. This includes processing required to open and maintain your account, provide our products and services, process transactions, deliver requested services, and fulfill our obligations under any agreement between you and Unipaynet. Certain personal information is essential for us to provide our services, and failure to provide such information may prevent us from delivering some or all of our products and services.
Compliance with Legal and Regulatory Obligations	We process personal data where required to comply with applicable laws, regulations, regulatory requirements, or lawful instructions from competent authorities. As a financial services provider, Unipaynet is required to collect, verify, retain, and process certain customer information to meet obligations relating to Know Your Customer (KYC), Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), fraud prevention, sanctions screening, tax compliance, and other regulatory requirements.
Legitimate Interests	We may process your personal data where necessary to pursue our legitimate business interests or those of relevant third parties, provided that such interests do not override your fundamental rights, freedoms, and privacy interests. Our legitimate interests may include improving our products and services, maintaining the security and reliability of our platforms, preventing fraud and financial crime, managing operational risks, enhancing customer experience, and developing new features and services.

Substantial Public Interest	In certain circumstances, Unipaynet may process personal data, including sensitive personal data where applicable, where such processing is necessary for reasons of substantial public interest and permitted by law. This may include complying with government requirements, supporting regulatory initiatives, protecting customers and the financial system, and providing appropriate support to customers who may be vulnerable or require additional assistance.
Consent	We may process your personal data where you have provided explicit and informed consent for a specific purpose. For example, we may request your consent before collecting optional information such as location data, accessing certain device features, or sending marketing communications. Where processing is based on your consent, you have the right to withdraw your consent at any time. Withdrawal of consent will not affect the lawfulness of any processing carried out before the withdrawal.

Unipaynet will ensure that all personal data processing activities are limited to what is necessary, relevant, and proportionate for the purpose for which the information was collected. We will also maintain appropriate safeguards to protect your personal data and respect your rights as a data subject.

Where multiple legal bases apply to the same processing activity, Unipaynet will determine and apply the most appropriate lawful basis based on the specific circumstances and applicable legal requirements.

6. How and Why We Use Your Personal Data

Unipaynet processes your personal data only for specific, lawful, and legitimate purposes. We use your information to provide our products and services, comply with legal and regulatory obligations, protect our customers and systems, prevent fraud, improve our services, and deliver a secure and personalized experience.
The table below explains the purposes for which we may process your personal data and the legal basis we rely on for such processing.

Purpose of Processing	How We Use Your Personal Data	Legal Basis for Processing
Providing and Managing Our Services	We use your personal data to provide, operate, and manage Unipaynet products and services. This includes verifying your identity through our Know Your Customer (KYC) processes, assessing eligibility for our services, opening and managing accounts, processing payments, facilitating deposits, withdrawals, transfers, electronic money transactions, and fulfilling our contractual obligations.	**Contractual Necessity** – Processing is required to provide the services you have requested and fulfill our obligations under our agreement with you. **Legal Obligations** – Processing is necessary to comply with applicable financial, regulatory, and compliance requirements.
Customer Support and	We use your information to provide customer support, respond to inquiries, resolve complaints, verify	**Contractual Necessity** – To provide customer

Service Management	instructions, maintain communication records, and monitor service interactions for quality assurance, training, security, and service improvement purposes.	support services associated with your account. **Legitimate Interests** – To maintain service quality, security, and operational efficiency.
Fraud Prevention and Financial Crime Management	We process personal data to verify your identity, detect suspicious activities, prevent fraud, manage security risks, comply with financial crime prevention requirements, and protect your account and the wider financial ecosystem.	**Legal Obligations** – To comply with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), sanctions, and other regulatory requirements. **Legitimate Interests** – To protect our customers, systems, and services against fraud and misuse.
Risk Assessment and Account Protection	We may analyze account activity, transaction patterns, and customer information to identify risks, prevent unauthorized transactions, and maintain the security and integrity of our services.	**Legitimate Interests** – To protect customers and maintain secure financial services. **Legal Obligations** – Where required by financial regulations.
Personalized Services and Customer Experience	We use information about your account, preferences, transactions, and service usage to personalize your experience, provide relevant features, recommend suitable products, and improve how our services meet your needs.	**Consent** – Where required, we will obtain your consent before using personal data for personalization activities. **Legitimate Interests** – To improve customer experience and develop better services.
Marketing and Promotional Communications	Where permitted by law, we may use your personal data to provide information about Unipaynet products, services, promotions, offers, and updates that may be relevant to you. We may also measure the effectiveness of marketing campaigns and improve our communications.	**Consent** – Where required, we will only send marketing communications after obtaining your permission. You may withdraw your consent or unsubscribe

		from marketing communications at any time.
Partner Offers and Third-Party Promotions	Where you have provided permission, we may share information with selected partners or provide information about third-party products, services, promotions, or offers that may be relevant to you.	**Consent** – Processing is based on your explicit permission where required by law.
Operating and Maintaining Our Platforms	We use personal data to manage, maintain, secure, and improve our website, mobile application, USSD platform, and other digital services. This includes troubleshooting, testing, analytics, research, system monitoring, and improving platform performance.	**Contractual Necessity** – To provide and maintain requested services. **Legitimate Interests** – To operate secure, reliable, and efficient digital platforms. **Consent** – Where required by applicable law.
Security and Authentication	We use personal data to verify your identity when accessing our services, contacting customer support, or performing sensitive activities on your account.	**Legal Obligations** – To comply with security and identity verification requirements. **Legitimate Interests** – To protect customer accounts and prevent unauthorized access.
Social and Connected Features	Where available and where you provide permission, we may use information from your device, such as contact lists, to enable social payment features, simplify transactions, or provide enhanced functionality.	**Consent** – Required before accessing information stored on your device, such as contacts or location information. **Legitimate Interests** – To improve and develop our services.
Location-Based Services	If you enable location permissions, we may use location information to support specific features, verify transactions, detect unusual activity, improve security, and prevent fraud.	**Consent** – Where you provide permission for location access. **Contractual Necessity** – Where location information is required to provide a requested service. **Legitimate Interests** – To

		protect customers and prevent fraudulent activity.
Analytics and Statistical Reporting	We may create aggregated or anonymized datasets to analyze customer behavior, improve services, conduct research, prepare reports, and meet regulatory reporting requirements. These datasets are processed in a manner that prevents identification of individual customers.	**Legal Obligations** – Where reporting is required by regulators or authorities. **Legitimate Interests** – To conduct analysis, research, and improve business operations.
Product and Service Improvement	We use customer insights, usage patterns, and feedback to develop new products, improve existing services, enhance functionality, and provide better customer experiences.	**Legitimate Interests** – To understand customer needs and continuously improve our services.
Compliance, Legal Enforcement, and Protection of Rights	We may process and disclose personal data where necessary to comply with legal requirements, respond to government or law enforcement requests, enforce agreements, recover outstanding obligations, defend legal claims, prevent crime, and protect our rights, customers, and business operations.	**Legal Obligations** – To comply with applicable laws and regulatory requirements. **Legitimate Interests** – To protect our legal rights and manage disputes. **Substantial Public Interest** – Where processing is necessary for regulatory, safety, or public protection purposes.

6.1 Processing Information Relating to Other Individuals

In certain circumstances, we may require information about other individuals connected to your transactions or use of our services. For example, we may request information about:

- A sender or recipient of funds.
- A beneficiary receiving payments.
- The source or origin of funds transferred into your account.
- Individuals involved in a transaction where additional verification is required.

You are responsible for ensuring that any information you provide about another person is accurate and that you have the necessary authority to provide such information.

6.2 Processing Data on Behalf of Business Customers

Where Unipaynet provides payment processing or business solutions to organizations, we may process personal data belonging to those organizations' customers, employees, or users.

In such circumstances:

- The business customer may act as the **Data Controller** responsible for determining why and how personal data is processed.
- Unipaynet may act as a **Data Processor** processing personal data only according to documented instructions from the business customer and applicable data protection laws.
- Both parties are responsible for ensuring that personal data is handled securely and lawfully within their respective roles.

Unipaynet remains committed to ensuring that all personal data processing activities are conducted transparently, securely, and in accordance with applicable data protection requirements.

7. Automated Decision-Making and Profiling

Depending on the Unipaynet products, services, and features you use, we may use automated processing technologies to support certain decisions relating to your account, transactions, and use of our services.
Automated processing involves the use of technology to analyze personal data, identify patterns, assess risks, and make decisions based on predefined criteria. This process may include **profiling**, which means evaluating aspects of your personal circumstances, behavior, transactions, or activities to predict potential risks, eligibility, or outcomes.

We use automated decision-making and profiling to improve the efficiency, security, and reliability of our services, ensure consistent decision-making, reduce operational errors, prevent fraud, and support compliance with applicable laws and regulations.

Where we make decisions solely through automated means that produce legal or similarly significant effects, you have the right, where applicable under data protection laws, to:

- Request human review of the decision.
- Request an explanation of the decision-making process.
- Challenge the outcome of the decision.
- Provide additional information relevant to the review.

Automated processing may be used in the following areas:

Activity	Use of Automated Processing
Customer Onboarding and Account Opening	Automated checks may be used during customer registration and onboarding, including identity verification, Know Your Customer (KYC) checks, Anti-Money Laundering (AML) screening, Politically Exposed Person (PEP) checks, sanctions screening, and address verification.
Transaction Monitoring and Management	Automated systems may analyze transactions to verify activity, apply transaction limits, assess risk levels, support transaction approvals, and identify unusual or suspicious activities.
Fraud Detection and Prevention	We use automated tools to monitor account activity, detect suspicious behavior, identify potential fraud patterns, prevent unauthorized transactions, and protect customers from financial crime.
Credit and Financial Assessment (Where Applicable)	Where Unipaynet provides credit-related products or services, automated systems may be used to assess applications, evaluate affordability, determine eligibility, establish limits, and support responsible lending decisions.
Account and Service Monitoring	Automated analysis may be used to monitor service usage, assess customer risk, maintain account security, and take appropriate actions where required to protect customers and comply with regulatory obligations.

The legal bases we rely on when conducting automated processing may include:

Legal Basis	Description
Contractual Necessity	Where automated processing is required to provide requested services, manage accounts, process transactions, or fulfill contractual obligations with you.
Legal Obligations	Where automated processing is necessary to comply with financial regulations, fraud prevention requirements, AML/CTF obligations, sanctions requirements, or other legal duties.
Legitimate Interests	Where automated processing supports our legitimate interests, including improving security, preventing financial crime, managing risks, and enhancing the efficiency and reliability of our services.
Consent	Where applicable laws require your consent before certain automated processing activities are carried out.

8. Marketing and Communications

Unipaynet may use your personal data to provide information about our products, services, features, offers, promotions, and other updates that may be relevant to you.

Where permitted by applicable laws, we may communicate with you through various channels, including:

- Email.
- SMS or text messages.
- Push notifications through the Unipaynet application.
- Telephone communications.
- Other digital communication channels.

Where consent is required, we will obtain your explicit permission before sending marketing communications or using your personal data for specific marketing purposes.

8.2 Personalized Marketing

To provide more relevant communications, we may analyze information such as:

- Your use of Unipaynet products and services.
- Your transaction history.
- Your account preferences.
- Your interactions with our digital platforms.

This may allow us to tailor communications, recommend relevant services, and improve your overall customer experience.

Where profiling is used for marketing purposes, you have the right to object to such processing and request that your marketing preferences be updated.

You may manage your communication preferences or stop receiving marketing messages at any time by:

- Selecting the unsubscribe option provided in our marketing communications.
- Updating your preferences through the Unipaynet application.
- Contacting our customer support team.

After you opt out of receiving personalized marketing communications, we may continue to provide essential service-related communications, such as security alerts, transaction notifications, regulatory updates, and information necessary to manage your account.

8.2 Sharing Personal Data for Marketing

Unipaynet will not sell, rent, or share your personal data with third parties for their independent marketing purposes without obtaining your explicit consent, unless permitted or required by applicable law.

8.3 Legal Basis for Marketing Activities

The legal bases we rely on when processing personal data for marketing purposes include:

Legal Basis	Description
Consent	Where required by law, we will obtain your clear and informed consent before sending marketing communications or conducting certain marketing activities. You may withdraw your consent at any time.
Legitimate Interests	We may process personal data for direct marketing where it is necessary to promote our services, improve customer engagement, and develop relevant offerings, provided that your privacy rights and expectations are respected. You have the right to object to this processing at any time.

Unipaynet is committed to ensuring that you remain in control of your personal data and marketing preferences. We will always provide transparency regarding how your information is used and respect your choices regarding communications.

9. Your Data Protection Rights

As an individual whose personal data is processed by Unipaynet, you have certain rights under applicable data protection and privacy laws. We are committed to respecting these rights and providing appropriate mechanisms for you to exercise control over your personal information.

The table below explains your rights and how they apply:

Your Right	What This Means
Right to be Informed	You have the right to understand how Unipaynet collects, uses, stores, and protects your personal data. This Privacy Notice explains our data processing practices, including the purposes for which we use your information and the legal basis for processing.
Right of Access to Your Personal Data	You have the right to request a copy of the personal data we hold about you and information about how we process it. However, we may not provide certain information where disclosure would affect the rights of another person, interfere with legal proceedings, compromise fraud or criminal investigations, or disclose confidential legal communications.
Right to Rectification (Correction of Personal Data)	You have the right to request correction of personal data that you believe is inaccurate, incomplete, outdated, or incorrect. Before making changes, we may take reasonable steps to verify the accuracy of the updated information provided.
Right to Erasure (Right to Delete Personal Data)	You may request the deletion of your personal data in certain circumstances, including where: • The information is no longer necessary for the purpose it was collected. • You withdraw consent and there is no other lawful basis for processing. • You successfully object to the processing of your data.

	• Your personal data has been processed unlawfully. • Applicable law requires the information to be deleted. However, as a regulated financial services provider, Unipaynet may be required to retain certain personal information to comply with legal, regulatory, fraud prevention, tax, accounting, or financial crime obligations. Where we cannot fulfill a deletion request, we will explain the reason and inform you of the applicable legal requirements.
Right to Object to Processing	You have the right to object to certain types of processing of your personal data, including processing based on legitimate interests and profiling activities related to marketing. If we have a compelling legal or operational reason to continue processing your information, we may refuse your objection. Where the processing is necessary to provide our services, exercising this right may affect our ability to continue providing certain products or services to you.
Right to Restrict Processing	You may request that we limit or temporarily suspend the processing of your personal data in certain circumstances, including where: • You believe your information is inaccurate and we are verifying it. • The processing is unlawful, but you do not want your data deleted. • We no longer need the information, but you require it for legal claims. • You have objected to processing and we are reviewing whether our legitimate interests override your request.
Right to Data Portability	Where applicable and technically feasible, you have the right to request your personal data in a structured, commonly used, and machine-readable format. You may also request that your data is transferred directly to another service provider where this is legally permitted and technically possible.
Right to Withdraw Consent	Where we process your personal data based on your consent, you have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before your withdrawal. To withdraw consent, you may contact us using the details provided in this Privacy Notice.
Right to Human Review of Automated Decisions	Where Unipaynet uses automated decision-making processes that produce legal or similarly significant effects, you have the right, where applicable, to request a review of the decision by a qualified person, provide additional information, and challenge the outcome.

9 Exercising Your Rights

To exercise any of your data protection rights, you may contact our Data Protection Officer using the following details:

Data Protection Officer

Email: data@unipaynet.com

When submitting a request, we may ask you to provide sufficient information to verify your identity and ensure that your personal data is disclosed only to the authorized individual.

9.1 Response Time and Limitations

Unipaynet will respond to your request within the timeframe required by applicable data protection laws, typically within **one month** from the date we receive a valid request.

In certain circumstances, this period may be extended where requests are complex or involve multiple requests. If an extension is required, we will notify you and explain the reason for the delay.

Your ability to exercise certain rights may be subject to legal and regulatory limitations. For example, financial services providers are required to retain certain customer information for specific periods to comply with obligations relating to financial crime prevention, regulatory reporting, taxation, audits, and record keeping.

Where we are unable to fully comply with your request, we will provide an explanation of the reasons and inform you of any available options or remedies.

10. Exercising Your Data Protection Rights

Unipaynet is committed to respecting your privacy rights and providing transparent mechanisms through which you can exercise control over your personal data.

If you wish to exercise any of the rights described in this Privacy Notice, you may submit your request through the Unipaynet mobile application or contact our Data Protection Officer using the following details:

Data Protection Officer

Email: data@unipaynet.com

10.1 Identity Verification

To protect your privacy and prevent unauthorized access to personal information, Unipaynet is required to verify your identity before processing any request relating to your personal data.

We may request additional information or supporting documentation, such as a government-issued identification document or other verification details, to confirm that you are the person entitled to make the request.

Where you are unable to provide sufficient proof of identity, we reserve the right to decline or delay processing your request until appropriate verification has been completed.

If a request is submitted by another person on your behalf, that individual must provide valid evidence of authorization, such as:

- A written authorization from you.
- A legally recognized power of attorney.
- Documentation confirming their authority to act on your behalf.

10.2 Processing Timeframes

Unipaynet aims to respond to valid data protection requests within the period required by applicable data protection laws, generally within **one (1) month** from the date the request is received.

Where a request is complex, involves multiple requests, or requires additional investigation, we may extend the response period as permitted by law. In such cases, we will notify you of the reason for the delay and keep you informed of the progress of your request.

10.3 Fees for Requests

You may exercise your data protection rights free of charge in most circumstances.
However, where a request is clearly unfounded, excessive, repetitive, or requires disproportionate resources, Unipaynet may charge a reasonable administrative fee or refuse to act on the request where permitted by law. We will notify you of any applicable fee before proceeding.

10.4 Complaints and Regulatory Rights

If you are dissatisfied with how Unipaynet has handled your request or believe that your data protection rights have not been properly addressed, you have the right to lodge a complaint with the relevant data protection authority in your jurisdiction.
For assistance regarding your privacy rights or the process for submitting a request, please contact us through the details provided above.

11. Sharing Your Personal Data

Unipaynet may share your personal data with selected recipients where necessary to provide our services, operate our business, comply with legal obligations, protect our customers, or improve our products and services.
We only share personal data where there is a lawful basis for doing so and take appropriate measures to ensure that your information remains secure and confidential.

11.1 Sharing Within the Unipaynet Group

Where applicable, your personal data may be shared between Unipaynet group entities for purposes including:

Purpose	Reason for Sharing
Providing products and services	To enable efficient delivery, management, and support of Unipaynet services
Customer support and account management	To ensure consistent service delivery and customer assistance across Unipaynet entities
Product improvement and development	To analyze service usage and improve customer experience
Communication about Unipaynet products and services	To provide relevant information about products, features, offers, and updates where permitted by law

Such sharing is based on applicable legal grounds, including legitimate business interests, contractual necessity, legal obligations, or your consent where required.

11.2 Sharing Information With Other Unipaynet Customers

Certain Unipaynet features may allow customers to discover and interact with other users of our services.

For example, where you provide permission, Unipaynet may access your mobile contacts to help identify which contacts are already using Unipaynet and make wallet-to-wallet transactions easier.

Feature	Privacy Controls
Contact synchronization	Available only after you provide explicit permission
Identifying Unipaynet users in your contacts	Limited information is displayed to support payment functionality

Contact access	You may disable access at any time through your device settings

This feature is optional, and you may withdraw your permission at any time by disabling contact access.

11.3 Sharing Information With Payment Recipients and Senders

When you send or receive payments through Unipaynet, we may share certain transaction-related information with the relevant parties to complete and verify the transaction.

The information shared is limited to what is necessary and may include:

Transaction Type	Information Shared
Sending payments	Your name, transaction reference details, and other information required to complete the payment
Receiving payments	Your name, account details, IBAN or equivalent payment identifiers where applicable, and information necessary to confirm the correct recipient

Such sharing enables secure payment processing, prevents errors, and helps comply with applicable financial regulations.

11.4 Sharing Information With Service Providers and Partners

Unipaynet works with carefully selected third-party service providers who support the delivery, security, and operation of our services.
These providers are required to maintain confidentiality, implement appropriate security measures, and process personal data only according to documented instructions and applicable laws.

Type of Service Provider	Purpose of Sharing Personal Data
Technology, IT infrastructure, and service providers	To maintain, operate, secure, and improve our platforms and systems
Payment processors, banking partners, and financial institutions	To process transactions, facilitate payments, provide financial services, and support payment networks
Card issuing, personalization, and delivery providers	To create, personalize, and deliver Unipaynet payment cards where applicable
Analytics and research providers	To analyze service performance, understand user behavior, and improve our products
Communication service providers	To deliver emails, SMS messages, push notifications, and other service communications
Identity verification and fraud prevention providers	To support KYC verification, security checks, fraud prevention, and regulatory compliance

11.5 Sharing Personal Data for Legal and Regulatory Reasons

Unipaynet may disclose personal data to authorized third parties where necessary to:

- Comply with applicable laws, regulations, court orders, or lawful requests from authorities.
- Support regulatory reporting obligations.

- Prevent, detect, investigate, or respond to fraud, money laundering, terrorism financing, or other financial crimes.
- Protect the rights, property, safety, and security of Unipaynet, our customers, or third parties.
- Establish, exercise, or defend legal claims.

We only disclose information where there is a valid legal basis and where such disclosure is necessary and proportionate.

11.6 Sharing Personal Data at Your Request

You may instruct Unipaynet to share your personal data with a third party where permitted by law.
Examples include authorizing:

- A lawyer or legal representative.
- An accountant or financial advisor.
- A guardian or authorized representative.
- A person acting under a valid power of attorney.

Before sharing your information, we may require evidence confirming that the third party has valid authorization to act on your behalf.

11.7 Unintended or Incorrect Transfers

In certain situations, Unipaynet may need to share limited information with another financial institution, service provider, or customer where necessary to resolve an incorrect payment, investigate an error, recover funds, or comply with legal obligations.
Any such disclosure will be handled carefully, limited to the information necessary for the purpose, and carried out with appropriate safeguards to protect your privacy.

11.8 Your Control Over Data Sharing

You have the right to understand how your personal data is shared and to object to certain processing activities where permitted by law.
If you have concerns regarding the sharing of your personal data, or if you would like further information about how your information is disclosed, please contact our Data Protection Officer:
Email: data@unipaynet.com
Unipaynet remains committed to ensuring that personal data is shared responsibly, securely, and only for legitimate purposes.

12. Where We Store and Transfer Your Personal Data

Unipaynet stores and processes personal data in secure locations, including within the country where the information is collected and in other jurisdictions where we or our trusted service providers operate.
Due to the nature of our international payment and financial services, your personal data may need to be transferred, accessed, or processed outside your country of residence. This may occur where necessary to facilitate international transactions, provide our services, maintain our technology infrastructure, or work with trusted service providers.
For example, where you make an international payment or transfer funds across borders, certain transaction-related information may need to be shared with financial institutions, payment networks, or service providers located in other countries.

12.1 Protection of Personal Data During International Transfers

Where personal data is transferred to countries that may not provide the same level of data protection as your country of residence, Unipaynet implements appropriate safeguards to ensure that your information remains protected.

These safeguards may include:

- Entering into appropriate data transfer agreements with third parties.
- Implementing contractual protections and confidentiality obligations.
- Applying technical and organizational security measures.
- Using recognized international transfer mechanisms where required by applicable law.

Where applicable, Unipaynet may rely on approved contractual safeguards, including Standard Contractual Clauses (SCCs) or other legally recognized transfer mechanisms, to ensure that international transfers comply with applicable data protection requirements.

You may request further information regarding the safeguards used for international data transfers by contacting our Data Protection Officer.

Email: data@unipaynet.com

Where appropriate, we may provide copies of relevant transfer safeguards, subject to necessary limitations to protect confidential information, security measures, or third-party rights.

12.2 Legal Basis for International Data Transfers

International transfers of personal data may be conducted where necessary for:

- Performing our contractual obligations with you.
- Taking steps requested by you before entering into a contract.
- Complying with legal and regulatory obligations.
- Protecting our legitimate business interests.
- Other lawful purposes permitted under applicable data protection laws.

13. Data Security

At Unipaynet, we recognize that protecting your personal data is a fundamental responsibility. We are committed to maintaining strong security controls designed to safeguard your information against unauthorized access, loss, misuse, alteration, disclosure, or destruction.

We implement appropriate technical, organizational, and physical security measures to protect the confidentiality, integrity, and availability of personal data.

Our security measures include:

Security Measure	Description
Access Controls	Restricting access to personal data only to authorized personnel who require it to perform their responsibilities.
Encryption and Secure Communication	Protecting data transmitted through our website, mobile application, and digital platforms using secure encryption technologies such as Transport Layer Security (TLS).
System Security	Maintaining secure infrastructure, databases, and technology systems designed to prevent unauthorized access and cyber threats.
Monitoring and Detection	Monitoring systems and activities to identify, investigate, and respond to suspicious or unauthorized behavior.

Employee Training	Providing regular privacy and information security training to employees and requiring compliance with internal security policies.
Data Protection Procedures	Maintaining policies and procedures governing the collection, storage, processing, and disposal of personal data.

In the event of a personal data breach, Unipaynet maintains incident response procedures to promptly identify, investigate, contain, and address security incidents.
Where required by applicable law, we will notify affected individuals and relevant regulatory authorities within the required timeframe.

13.1 Protecting Your Account Information

The security of your Unipaynet account also depends on your actions. You are responsible for keeping your passwords, PINs, authentication details, and account credentials confidential.
You should:

- Avoid sharing your login credentials with anyone.
- Use strong and unique passwords.
- Enable available security features.
- Immediately notify Unipaynet if you suspect unauthorized access or suspicious activity.

Unipaynet continuously reviews and improves its security practices to address evolving cybersecurity risks and technological developments.

14. How Long We Retain Your Personal Data

Unipaynet retains personal data only for as long as necessary to fulfill the purposes for which it was collected, comply with legal and regulatory obligations, resolve disputes, enforce agreements, and protect our legitimate interests.
The retention period for personal data depends on factors including:

- The type and sensitivity of the information.
- The purpose for which it was collected.
- Our contractual obligations.
- Applicable legal and regulatory requirements.
- Requirements relating to financial records, fraud prevention, audits, and legal claims.

As a regulated financial services provider, Unipaynet may be required to retain certain customer information for a specified period after the termination of your relationship with us.
In general, personal data may be retained for a period required by applicable laws, which may include obligations relating to:

- Anti-Money Laundering (AML).
- Counter-Terrorist Financing (CTF).
- Tax reporting.
- Financial audits.
- Regulatory investigations.
- Legal claims and dispute resolution.

We regularly review our retention practices to ensure that personal data is not retained longer than necessary.

Once the applicable retention period expires, personal data will be securely deleted, destroyed, or anonymized unless continued retention is required by law or necessary for legitimate purposes.
You may request deletion of your personal data where applicable under your legal rights. However, certain information may be retained where legal obligations require us to do so.
For questions regarding data retention periods or to exercise your rights, contact:
Email: data@unipaynet.com

15. Changes to This Privacy Notice

Unipaynet is committed to maintaining transparency regarding how we collect, use, and protect personal data.
We may update this Privacy Notice from time to time to reflect:

- Changes to our products and services.
- Changes in applicable laws and regulations.
- Improvements to our privacy practices.
- Changes in how we process personal data.

Where significant changes are made that materially affect your privacy rights or how we process your personal data, we will provide appropriate notification through channels such as:

- Email communications.
- The Unipaynet mobile application.
- Our official website.
- Other appropriate communication methods.

For minor updates that do not significantly affect your rights, we may update this Privacy Notice and publish the revised version on our website.
Where a change introduces new processing activities requiring your consent, we will obtain your consent before carrying out such processing.
We encourage you to review this Privacy Notice periodically to remain informed about how Unipaynet protects and uses your personal data.

16. Cookies and Similar Technologies

Unipaynet uses cookies and similar technologies to improve user experience, enhance website functionality, analyze usage patterns, strengthen security, and support our marketing activities.
Cookies are small data files stored on your device when you visit our website. They help us remember preferences, understand how users interact with our platforms, and improve our services.
Detailed information about the cookies we use, their purposes, and retention periods is available in our **Cookie Policy**.

16.1 Managing Cookie Preferences

When you first visit our website, we may request your consent before placing non-essential cookies on your device.
You may choose to:

- Accept all cookies.
- Reject non-essential cookies.
- Customize your preferences by selecting specific cookie categories.

You can change your cookie preferences at any time through our Cookie Settings or your browser settings.

16.2 Types of Cookies We May Use

Cookie Category	Purpose
Essential Cookies	Required for website functionality, security, authentication, and basic services.
Functional Cookies	Used to remember preferences and improve user experience.
Analytics Cookies	Used to understand website usage, improve performance, and analyze customer interactions.
Marketing Cookies	Used to provide relevant advertising and measure marketing effectiveness where permitted.

16.3 Email Tracking Technologies

Our marketing communications may contain technologies such as tracking pixels or web beacons that help us understand campaign performance.

These technologies may allow us to determine:

- Whether an email was delivered.
- Whether an email was opened.
- Whether links within an email were accessed.
- Technical information such as IP address, browser type, and email client.

You may prevent email tracking by:

- Unsubscribing from marketing communications.
- Adjusting your email application settings.
- Blocking automatic image loading.

16.4 Third-Party Cookies

We may use trusted third-party service providers that place cookies or similar technologies on our platforms to support analytics, security, performance improvements, and advertising activities.

Information about managing third-party cookies is available through our Cookie Policy.

Our use of strictly necessary cookies is based on our legitimate interests in ensuring that our website and services operate securely and effectively.

For cookies that require consent under applicable laws, Unipaynet will obtain your permission before activating them.