

Banxa | EU Privacy Notice Addendum

Effective: 1 January 2026

Last Updated: 1 January 2026

Table of Contents

2. NOTICE AT COLLECTION	2
2A. Data Minimization Justification	2
2B. Ongoing Review and Minimization	5
3. HOW WE USE YOUR PERSONAL DATA	6
3A. Legitimate Interests Balancing	6
3B. Detailed Automated Decision-Making Information	8
4. JOINT CONTROLLER ARRANGEMENTS	9
4A. When Joint Controller Arrangements Apply	9
4B. Key Joint Controller Relationships	9
4C. Essence of Joint Controller Arrangements	10
4D. Your Rights Under Joint Controller Arrangements	10
4E. Complete Joint Controller Arrangements	10
7. YOUR PRIVACY CHOICES AND RIGHTS	10
7A. Right to Object	10
7B. Consent Withdrawal Mechanisms	13
14. BLOCKCHAIN-SPECIFIC GDPR COMPLIANCE	16

PRIVACY NOTICE SUMMARY

This is a summary of our key privacy practices. For full details, please read the complete information notice below.

Who we are: Banxa is a cryptocurrency on-ramp/off-ramp service provider. The specific Banxa entity acting as data controller depends on your location.

What information we collect: Identity information, financial data, transaction details, technical data, and in some cases biometric data for verification.

Why we use it: To provide our services, comply with legal obligations (anti-money laundering, tax laws), prevent fraud, and improve our services.

Your key rights: Access, correction, deletion, objection, portability, and consent withdrawal.

Your right to object: You have the right to object to processing based on our legitimate interests, including for direct marketing purposes.

Contact us: privacy@banxa.com

In accordance with Article 37 of the General Data Protection Regulation (GDPR), Banxa has appointed a Data Protection Officer (DPO) to oversee our data protection strategy and compliance with applicable Personal Data Protection laws.

Data Protection Officer Contact Information:

Name: Rui Serrano

Email: dpo@banxa.com

Postal Address: Azeitao, Portugal

You may contact our DPO regarding:

- Questions about how your Personal Data is processed
- Concerns about data protection practices
- Exercise of your data subject rights
- Data protection compliance matters
- Filing complaints about our data processing activities

Our DPO works independently to ensure Banxa's compliance with applicable Personal Data Protection laws and serves as a point of contact with supervisory authorities.

2. NOTICE AT COLLECTION

2A. Data Minimization Justification

Under Article 5(1)(c) GDPR, we are required to ensure that personal data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (data minimization principle).

Below is our justification for each category of Personal Data we collect, explaining why it is necessary and proportionate:

2A1. Government-Issued Identification Documents

What we collect: Passport, driver's license, national ID card

Why necessary:

- **Legal Requirement:** AML/CTF regulations in all jurisdictions where we operate require us to verify customer identity using government-issued photo ID
- **Fraud Prevention:** Photo ID is the most reliable method to prevent identity theft and synthetic identity fraud
- **Age Verification:** Required to ensure users meet minimum age requirements (18+ in most jurisdictions)
- **Proportionality:** We collect only one primary ID document; additional documents only requested if first is insufficient

Alternatives Considered: Self-certification or lower-evidence methods do not meet regulatory standards for financial services.

2A2. Biometric Facial Recognition Data

What we collect: Facial biometric templates extracted from selfie photos

Why necessary:

- **Enhanced Identity Verification:** Comparing facial biometrics between ID and live selfie provides strong authentication against photo substitution fraud
- **Regulatory Requirement:** Some jurisdictions require liveness detection and facial matching for cryptocurrency service providers
- **Fraud Prevention:** Biometric matching detects account takeover attempts and prevents identity theft
- **Proportionality:** Biometric data is processed only with explicit consent or legal requirement; deleted within 1 year; used solely for verification, not other purposes

Alternatives Considered: Manual document review is less secure and scalable; knowledge-based authentication is vulnerable to fraud; biometric matching provides best balance of security and user experience.

2A3. Proof of Address (Utility Bills)

What we collect: Utility bills, bank statements showing residential address

Why necessary:

- **Regulatory Requirement:** Financial services regulations require proof of current address
- **Fraud Prevention:** Confirms genuine residence and prevents use of mail drops or fraudulent addresses
- **Sanctions Compliance:** Address verification is required to screen against sanctions and embargo jurisdictions
- **Proportionality:** We accept any standard utility bill or bank statement; document must be recent (typically within 3 months)

Alternatives Considered: Some jurisdictions accept electronic verification via databases, which we use where available; however, many jurisdictions require documentary evidence.

2A4. Financial Information (Bank Accounts, Cards)

What we collect: Bank account numbers, credit/debit card numbers, bank statements

Why necessary:

- **Service Delivery:** Essential to process fiat currency payments and transfers
- **Legal Requirement:** Payment service regulations require us to verify payment instruments
- **Fraud Prevention:** Prevents use of stolen payment methods
- **Chargeback Protection:** Bank information necessary for dispute resolution
- **Proportionality:** We collect only payment methods you choose to use; stored securely with PCI-DSS compliance for cards

Alternatives Considered: Cannot provide fiat on/off-ramp services without payment instrument information.

2A5. Transaction History and Sources of Funds

What we collect: Details of your transactions including amounts, purposes, sender/receiver, beneficial owners

Why necessary:

- **AML/CTF Legal Obligation:** "Travel Rule" regulations require us to collect and share transaction party information
- **Enhanced Due Diligence:** Regulatory requirements to verify source of funds for large or suspicious transactions
- **Sanctions Screening:** Required to ensure transactions don't involve sanctioned individuals or entities
- **Proportionality:** Information collected is proportionate to transaction value and risk; enhanced information only for higher-risk transactions

Alternatives Considered: Regulatory requirements are prescriptive; no viable alternatives exist.

2A6. Wallet Addresses and Blockchain Data

What we collect: Cryptocurrency wallet addresses, transaction history, wallet balances

Why necessary:

- **Service Delivery:** Essential to send/receive cryptocurrency
- **AML Compliance:** Required to monitor for suspicious blockchain activity
- **Sanctions Screening:** Wallet addresses must be screened against sanctions lists
- **Proportionality:** We collect only wallet addresses you use with our service; blockchain data is publicly available

Alternatives Considered: Cannot provide cryptocurrency services without wallet addresses.

2A7. Technical and Usage Data

What we collect: IP addresses, device information, usage patterns, cookies

Why necessary:

- **Security:** Essential for fraud detection, account security, DDoS protection
- **Service Delivery:** Technical data necessary for platform functionality
- **Legal Compliance:** Some jurisdictions require logging of access for security purposes
- **Proportionality:** Technical data retained only as long as necessary for security purposes (typically 24 hours to 2 years depending on purpose)

Alternatives Considered: Cannot operate secure online platform without collecting technical data; we minimize retention periods and use anonymization where possible.

2A8. Professional Details and Occupation

What we collect: Employment information, occupation, professional status

Why necessary:

- **Enhanced Due Diligence:** Required for Politically Exposed Persons (PEP) screening
- **Risk Assessment:** Certain occupations present higher risk under AML regulations (e.g., cash-intensive businesses)
- **Source of Funds Verification:** Employment helps verify legitimate income sources
- **Proportionality:** Basic occupation information only; detailed employment history not required

Alternatives Considered: This is a regulatory requirement for financial services; alternatives do not meet compliance standards.

2A9. National Insurance/Social Security Numbers

What we collect: Tax identification numbers, social security numbers (jurisdiction-dependent)

Why necessary:

- **Tax Reporting:** Legal obligation to report cryptocurrency transactions to tax authorities in many jurisdictions
- **Identity Verification:** Some jurisdictions require tax ID for definitive identity verification
- **Proportionality:** Only collected in jurisdictions where legally required or necessary for identity verification

Alternatives Considered: Collection is legally mandated in relevant jurisdictions.

2B. Ongoing Review and Minimization

We conduct regular reviews (at least annually) to:

- Assess whether data collection remains necessary

- Identify opportunities to reduce data collection
- Implement new privacy-enhancing technologies
- Respond to regulatory changes that may reduce requirements

Your Right to Challenge: If you believe any data we collect is not necessary, you may contact our DPO at dpo@banxa.com to raise your concerns. We will review and respond to all data minimization challenges.

3. HOW WE USE YOUR PERSONAL DATA

3A. Legitimate Interests Balancing

When we process your Personal Data based on our legitimate interests under Article 6(1)(f) GDPR, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms. Below are the key legitimate interests we rely on and our balancing assessment:

3A1. Direct Marketing of Similar Services (Soft Opt-In)

Our Legitimate Interest: Promoting services similar to those you have already purchased helps us maintain customer relationships and provide you with relevant service updates that may benefit your cryptocurrency trading activities.

Balancing Assessment:

- **Your Interests:** You have an interest in not receiving excessive marketing communications.
- **Balancing Factors:** We only market similar services; you can easily opt-out at any time via unsubscribe links; we do not market third-party products without explicit consent; communications are limited in frequency.
- **Safeguards:** Opt-out mechanism in every communication; suppression of opt-out requests within 48 hours; regular review of marketing preferences.
- **Conclusion:** Our interest in customer engagement does not override your rights given the narrow scope and easy opt-out.

3A2. Fraud Prevention and Network Security

Our Legitimate Interest: Protecting our platform, our users, and ourselves from fraud, security threats, and financial crime is essential to maintain trust and operational integrity.

Balancing Assessment:

- **Your Interests:** You have an interest in privacy and minimal data processing.
- **Balancing Factors:** Fraud prevention protects you from financial loss; it protects other users; it prevents criminal activity; financial services are high-risk for fraud; you benefit from a secure platform.
- **Safeguards:** Data access restricted to security personnel; automated systems with human oversight; regular security audits; data minimization in fraud detection systems.

- **Conclusion:** Fraud prevention is strongly in your interest as it protects your funds and identity, and the processing is proportionate to the fraud risks in cryptocurrency services.

3A3. Service Improvement and Development

Our Legitimate Interest: Analyzing how our Services are used allows us to improve user experience, fix technical issues, and develop new features that benefit all users.

Balancing Assessment:

- **Your Interests:** You have an interest in limiting analytical tracking.
- **Balancing Factors:** Service improvements benefit you directly; analysis uses aggregated/pseudonymized data where possible; insights help reduce friction and improve security.
- **Safeguards:** Analytics data is anonymized where possible; access restricted to product and engineering teams; retention limited to 2 years; no analytics used for individual profiling without consent.
- **Conclusion:** Service improvement is beneficial to you and uses the minimum data necessary for legitimate quality enhancement.

3A4. Research and Development (Including Marketing Research)

Our Legitimate Interest: Understanding market trends and customer needs helps us develop relevant services and remain competitive.

Balancing Assessment:

- **Your Interests:** You have an interest in not being subjected to unnecessary research.
- **Balancing Factors:** Research helps us develop services you may need; participation is often voluntary (surveys); data is typically anonymized for research purposes.
- **Safeguards:** Research data pseudonymized or anonymized; voluntary participation where possible; results used at aggregate level; opt-out available for marketing research.
- **Conclusion:** Research benefits outweigh minimal intrusion, particularly given anonymization and voluntary participation.

3A5. Internal Business Operations and Record Keeping

Our Legitimate Interest: Maintaining business records and conducting audits are necessary for operational efficiency, quality assurance, and demonstrating compliance.

Balancing Assessment:

- **Your Interests:** You have an interest in data minimization and limited retention.
- **Balancing Factors:** Records necessary for dispute resolution; audit trails protect both parties; some record keeping is required by law; records support your rights (e.g., proof of transactions).

- **Safeguards:** Records retained only as long as necessary; access restricted by role; regular data review and deletion; encryption of stored data.
- **Conclusion:** Record keeping is necessary for both parties' protection and is proportionate to legitimate business needs.

3A6. Legal Claims and Dispute Resolution

Our Legitimate Interest: Maintaining data necessary to establish, exercise, or defend legal claims protects our legal rights and enables fair dispute resolution.

Balancing Assessment:

- **Your Interests:** You have an interest in data deletion after service termination.
- **Balancing Factors:** Legal claims can arise years after a transaction; you may also need records to defend your own claims; limitation periods vary by jurisdiction.
- **Safeguards:** Data retained only for applicable limitation periods; access restricted to legal team; data archived (not in active systems); deleted after limitation period expires.
- **Conclusion:** Legal claim data retention is necessary for both parties to exercise legal rights and is limited to statutory limitation periods.

Your Right to Object

You have the right to object to processing based on legitimate interests at any time. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests, or the processing is necessary for legal claims.

3B. Detailed Automated Decision-Making Information

What Automated Decisions We Make:

1. **Fraud Risk Assessment:** Automated systems analyze transaction patterns, device fingerprints, and behavioral signals to assign risk scores that may result in transaction blocking or account suspension.
2. **Identity Verification:** Automated comparison of facial biometrics and document verification may result in account approval or denial.
3. **Transaction Limits:** Automated systems may impose transaction limits based on verification level and risk assessment.
4. **AML Screening:** Automated checks against sanctions lists and PEP databases may flag or block transactions.

Logic and Significance:

- **Risk Scoring Algorithm:** Uses machine learning models trained on fraud patterns, considering factors like transaction velocity, amounts, geographic locations, device characteristics, and blockchain analysis.
- **Significance:** These decisions can significantly affect you by denying service access or blocking transactions worth substantial amounts.

Your Rights Regarding Automated Decisions:

- Right to human review of automated decisions
- Right to express your point of view
- Right to contest the decision
- Right to obtain an explanation of the decision and the logic involved

How to Exercise These Rights: Contact us at dpo@banxa.com or privacy@banxa.com with subject line "Automated Decision Review Request." We will provide human review within 7 business days.

4. JOINT CONTROLLER ARRANGEMENTS

Banxa operates through multiple legal entities globally. In certain circumstances, more than one Banxa entity may act as a data controller for your Personal Data, making them joint controllers under Article 26 GDPR.

4A. When Joint Controller Arrangements Apply

Joint controller arrangements occur when:

1. You use Services that involve entities in different jurisdictions
2. Multiple Banxa entities are necessary to complete your transaction
3. Shared systems and infrastructure are used across Banxa entities
4. Compliance obligations require coordination between entities

4B. Key Joint Controller Relationships

i. EU/UK Operations:

- **Joint Controllers:** EU Internet Ventures B.V. (Netherlands) and BNXA UK VASP Limited (UK)
- **Purpose:** Providing services to UK and EEA customers
- **Arrangement:** EUIV BV operates primary platform; BNXA UK handles UK regulatory compliance
- **Your Point of Contact:** Both entities are jointly responsible; contact privacy@banxa.com

ii. Group-Wide Fraud Prevention:

- **Joint Controllers:** All Banxa entities share fraud prevention systems
- **Purpose:** Detecting and preventing fraud across the global platform
- **Arrangement:** Global Internet Ventures Pty Ltd maintains central fraud database; all entities contribute data and benefit from fraud signals
- **Your Point of Contact:** Entity in your jurisdiction; escalate to dpo@banxa.com

iii. Shared Technology Infrastructure:

- **Joint Controllers:** Primary operating entities in your region + Global Internet Ventures Pty Ltd (Australia)

- **Purpose:** Platform hosting, technical operations, data storage
- **Arrangement:** Global Internet Ventures Pty Ltd operates core technology infrastructure used by all Banxa entities
- **Your Point of Contact:** Contracting entity in your jurisdiction

4C. Essence of Joint Controller Arrangements

Where joint controller arrangements exist:

- **Joint Responsibility:** Each entity is responsible for GDPR compliance for the processing they perform
- **Primary Contact:** The Banxa entity in your jurisdiction is your primary contact for exercising rights
- **Data Sharing:** Personal Data may be shared between joint controllers as necessary for the purposes above
- **Coordination:** Joint controllers coordinate on data subject rights requests, security incidents, and regulatory matters

4D. Your Rights Under Joint Controller Arrangements

You may exercise your rights against any of the joint controllers. The entity you contact will coordinate with other joint controllers as needed to fulfill your request. You may also contact our Data Protection Officer at dpo@banxa.com who can coordinate across all Banxa entities.

4E. Complete Joint Controller Arrangements

For a complete description of joint controller arrangements, including the determination of respective responsibilities, contact: dpo@banxa.com

7. YOUR PRIVACY CHOICES AND RIGHTS

7A. Right to Object

Under Article 21 GDPR, you have important rights to object to certain types of data processing. This section explains these rights in detail and how to exercise them.

7A1. Article 21(1) - Right to Object to Processing Based on Legitimate Interests

You have the right to object at any time to processing of your personal data based on our legitimate interests (Article 6(1)(f)), including profiling based on those provisions.

When this right applies:

- Processing based on legitimate interests
- Profiling for service improvement or fraud prevention
- Research and development activities
- Business operations not strictly necessary for service delivery

How we will respond: We will stop processing your Personal Data unless we can demonstrate compelling legitimate grounds for the processing which override your interests,

rights and freedoms, or the processing is necessary for the establishment, exercise or defense of legal claims.

Examples of when we may continue processing:

- Fraud prevention processing where your account has exhibited suspicious activity patterns
- Security monitoring where we have evidence of potential security threats
- Legal claims where we need the data to defend against claims you have made

How to exercise this right:

1. Email: dpo@banxa.com or privacy@banxa.com
2. Subject line: "Objection to Processing - Article 21(1)"
3. Specify: Which processing activities you object to and your reasons
4. We will respond within 1 month

7A2. Article 21(2) - Right to Object to Direct Marketing (ABSOLUTE RIGHT)

When you object to direct marketing:

- We will stop processing your personal data for direct marketing purposes
- This applies to both direct marketing communications and profiling for direct marketing
- We will honor your objection immediately with no exceptions

What constitutes direct marketing:

- Promotional emails about our services
- SMS marketing messages
- Targeted advertising based on your profile
- Marketing phone calls
- Promotional push notifications

How to object to direct marketing:

1. **Email:** Click "unsubscribe" in any marketing email
2. **SMS:** Reply "STOP" to any marketing text message
3. **Phone:** Tell us during the call or call +1 800-909-9664
4. **General Opt-Out:** Email privacy@banxa.com with subject "Marketing Opt-Out"
5. **Account Settings:** Log in and update marketing preferences

We will process your objection within 48 hours for email/SMS and immediately for phone calls.

7A3. Article 21(3) - Information About Right to Object

In compliance with Article 21(3), we are explicitly informing you of your right to object:

- This right is clearly presented in this section
- You can exercise this right at any time
- No fees apply to exercise this right
- We will not discriminate against you for exercising this right

7A4. Article 21(4) - Direct Marketing Notice Requirement

This right is explicitly brought to your attention and presented clearly and separately from other information in this Privacy Notice.

7A5. Article 21(5) - Information Society Services

Where we provide information society services (online services) and you object to processing in the context of these services, you may exercise your right to object by automated means using technical specifications.

Technical opt-out methods available:

- Cookie consent management platform
- Account privacy settings
- Browser-based opt-out tools
- Email preference center (link provided in all marketing emails)

7A6. Article 21(6) - Scientific/Historical Research and Statistics

Where we process your data for scientific or historical research purposes or statistical purposes under Article 89(1), you have the right to object on grounds relating to your particular situation, unless the processing is necessary for a task carried out for reasons of public interest.

Current relevant processing:

- Market research and industry analysis (aggregated data)
- Service usage statistics and trends
- Historical transaction analysis for service improvement

How to object to research/statistical processing: Contact dpo@banxa.com with subject "Research Processing Objection" explaining your particular circumstances.

7A7. Consequences of Objection

Depending on what you object to, the following may occur:

If you object to marketing:

- You will stop receiving marketing communications
- We will not profile you for marketing purposes
- **No impact on service delivery**

If you object to legitimate interest processing:

- If we cannot demonstrate overriding legitimate grounds, we will cease processing
- This may impact certain service features (e.g., fraud detection)
- We will explain any service limitations before implementing your objection
- You may withdraw your objection to restore full functionality

If you object to research/statistics:

- Your data will be excluded from research datasets
- No impact on service delivery
- May be excluded from service improvement benefits

Escalation

If you are not satisfied with our response to your objection:

1. Contact our Data Protection Officer: dpo@banxa.com
2. File a complaint with your supervisory authority
3. Seek judicial remedy

7B. Consent Withdrawal Mechanisms

Where we process your personal data based on consent (Article 6(1)(a) or Article 9(2)(a) GDPR), you have the right to withdraw your consent at any time. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

7B1. How to Withdraw Consent by Processing Purposes

1. Marketing Communications Consent

What you consented to: Receiving promotional emails, SMS, or push notifications about Banxa services

How to withdraw:

- **Email:** Click "unsubscribe" in any marketing email (instant effect)
- **SMS:** Reply "STOP" to marketing text messages (instant effect)
- **Push Notifications:** Disable in mobile app settings or device settings
- **All Marketing:** Email privacy@banxa.com with subject "Withdraw Marketing Consent"
- **Account Portal:** Log in to your account and update communication preferences

Effect of withdrawal: You will stop receiving marketing communications within 48 hours. Transaction and service-related communications will continue as these are necessary for service delivery.

2. Biometric Data Processing Consent

What you consented to: Collection and processing of facial biometric data for identity verification

How to withdraw:

- **Email:** dpo@banxa.com with subject "Withdraw Biometric Consent"
- **Include:** Your account email and confirmation you wish to delete biometric data
- **Phone:** +1 800-909-9664 (mention biometric data deletion)

Effect of withdrawal: Your biometric data will be deleted within 48 hours. **Important:** You may need to complete alternative identity verification if you wish to continue using our services. We will contact you to discuss alternatives.

Timeline: Biometric data deletion confirmed within 5 business days.

3. Cookie and Tracking Consent

What you consented to: Non-essential cookies including analytics, functionality, and marketing cookies

How to withdraw:

- **Cookie Settings:** Click "Cookie Settings" in website footer and adjust preferences
- **Browser Settings:** Clear cookies and adjust browser privacy settings
- **Do Not Track:** Enable in browser (though we note we don't respond to DNT signals per Section 7)

Effect of withdrawal: Non-essential cookies will be deleted from your browser. Essential cookies required for service functionality will remain. Some features may be limited.

4. Precise Location Data Consent (Mobile App)

What you consented to: Collection of precise GPS location data through mobile app

How to withdraw:

- **iOS:** Settings > Privacy > Location Services > Banxa > Select "Never" or "While Using"
- **Android:** Settings > Apps > Banxa > Permissions > Location > Disable or select "Only when in use"
- **In-App:** App Settings > Privacy > Location Services > Disable

Effect of withdrawal: App will no longer collect precise location data. Some location-based features may be unavailable. We may still collect approximate location from IP address for fraud prevention (legitimate interest basis).

5. Profiling for Service Personalization Consent

What you consented to: Profiling your behavior and preferences to personalize service recommendations

How to withdraw:

- **Email:** privacy@banxa.com with subject "Withdraw Profiling Consent"
- **Account Settings:** Privacy Settings > Data Processing > Personalization > Disable

Effect of withdrawal: We will stop profiling you for personalization purposes. You will receive generic service experience. Fraud prevention profiling will continue based on legitimate interests.

6. Third-Party Data Sharing Consent

What you consented to: Sharing your data with specific third parties for joint marketing or specific purposes

How to withdraw:

- **Email:** privacy@banxa.com with subject "Withdraw Third-Party Sharing Consent" and specify which third parties
- **Account Settings:** Privacy Settings > Third-Party Sharing > Manage Consents

Effect of withdrawal: We will stop sharing your data with specified third parties for the consented purpose. Sharing required for service delivery (e.g., payment processors) will continue based on contract performance.

7. Research and Survey Participation Consent

What you consented to: Use of your data for research purposes or participation in surveys

How to withdraw:

- **Email:** privacy@banxa.com with subject "Withdraw Research Consent"
- **Survey Links:** Click "opt out of future surveys" in any survey invitation

Effect of withdrawal: You will be excluded from future research studies and surveys. Previously collected survey responses may remain in anonymized datasets where re-identification is impossible.

7B2. General Consent Withdrawal

To withdraw ALL consents simultaneously: Email privacy@banxa.com with subject "Withdraw All Consents" and we will:

1. Confirm all consents currently active on your account
2. Explain consequences of withdrawing each consent
3. Upon your confirmation, withdraw all consents within 48 hours
4. Provide written confirmation of completed withdrawals

Important Notes About Consent Withdrawal

Lawfulness of Past Processing: Withdrawing consent does not make our previous processing unlawful. We were entitled to process your data based on your consent up to the point of withdrawal.

Impact on Services: Some consents are necessary for us to provide certain services. Withdrawing these consents may result in:

- Inability to use certain features
- Need for alternative verification methods
- Potential service restrictions

We will always explain the consequences before processing your withdrawal.

Other Legal Bases: Even if you withdraw consent, we may continue processing your data if we have another legal basis (e.g., legal obligation, contract performance, legitimate interests). We will explain any continuing processing after consent withdrawal.

No Disadvantage: You will not face any disadvantage for withdrawing consent, except the natural consequences of us no longer processing data for that specific purpose.

Processing Timeline:

- **Immediate:** Marketing opt-outs, cookie withdrawals
- **48 hours:** Biometric data deletion, third-party sharing cessation
- **5 business days:** Complex consent withdrawals requiring system updates

Confirmation: We will always send written confirmation when we have processed your consent withdrawal, explaining what has been done and any continuing processing under other legal bases.

7C. REQUESTING LIST OF SERVICE PROVIDERS AND RECIPIENTS

You may request a complete list of our current service providers and recipients by contacting privacy@banxa.com. We update this list regularly and will provide the most current information upon request.

14. BLOCKCHAIN-SPECIFIC GDPR COMPLIANCE

Blockchain technology presents unique challenges for GDPR compliance due to its inherent characteristics of immutability and decentralization. This section explains how we address these challenges while respecting your data protection rights.

The Blockchain Challenge

Public blockchain networks (such as Ethereum, Bitcoin, and others) are:

- **Immutable:** Once data is recorded, it cannot be altered or deleted
- **Distributed:** Data is replicated across thousands of independent nodes globally
- **Permissionless:** Anyone can access and read public blockchain data
- **Decentralized:** No single entity controls the blockchain

These characteristics create tension with certain GDPR rights, particularly the right to erasure (Article 17) and the right to rectification (Article 16).

What Blockchain Data Involves Your Personal Data

The following blockchain data may qualify as Personal Data when linked to your identity:

1. **Wallet Addresses:** Cryptocurrency addresses you use with our Services
2. **Transaction Records:** On-chain transactions including amounts, timestamps, and counterparty addresses
3. **Token Balances:** Cryptocurrency and token holdings visible on public blockchains

4. **Smart Contract Interactions:** Records of your interactions with decentralized applications
5. **Metadata:** Transaction notes or memo fields (if used)

Important: While blockchain data is publicly visible, it becomes "personal data" under GDPR when we or others can link a wallet address to your real-world identity through our KYC records or other identifiers.

Our GDPR Compliance Approach for Blockchain Data

1. Data Minimization

We minimize the amount of personal data recorded on blockchains:

- **Off-Chain Identity:** We store your identity information (name, ID documents, biometric data) entirely off-chain in systems we control
- **Wallet Linkage:** We maintain the link between your identity and wallet addresses in our off-chain databases, not on the blockchain
- **No Personal Data on Blockchain:** We never write your name, email, ID numbers, or other obvious personal data directly onto any blockchain
- **Pseudonymous Addresses:** Wallet addresses are inherently pseudonymous and do not reveal your identity without additional linkage data

2. Right to Erasure - Practical Implementation

While we cannot delete data from public blockchains, we can effectively render it non-personal by breaking linkages:

What we CAN do when you request erasure:

- **Delete Identity Linkages:** Delete all off-chain records linking your identity to wallet addresses
- **Delete Off-Chain KYC Data:** Completely delete your identity documents, biometric data, and Personal Data from our systems
- **Delete Transaction Metadata:** Delete transaction purposes, beneficiary information, and other off-chain transaction details
- **Anonymize Account Records:** Remove your identity from account records, transaction histories, and logs in our systems
- **Break the Link:** After these deletions, your wallet addresses on the blockchain become practically anonymous again since no one (including us) can link them to you

What we CANNOT do:

- **Delete from Blockchain:** Cannot remove wallet addresses or transaction records from public blockchains (technically impossible)
- **Control Third Parties:** Cannot control what third parties (exchanges, wallets, blockchain analytics firms) may know about your addresses

The Practical Effect: After we process your erasure request:

1. Your identity is completely removed from our systems
2. The on-chain wallet addresses remain on the blockchain but are no longer linked to your identity
3. The addresses return to a pseudonymous state
4. Unless you've publicly disclosed your wallet addresses elsewhere, they cannot be traced back to you

This approach aligns with the European Data Protection Board (EDPB) guidance acknowledging that pseudonymization can satisfy erasure obligations when deletion is technically impossible.

3. Right to Rectification

Challenge: Blockchain transactions cannot be edited once confirmed.

Our Approach:

- **Off-Chain Correction:** We correct any incorrect Personal Data in our off-chain databases (your name, address, etc.)
- **Transaction Disputes:** For incorrect transaction records on the blockchain, we can:
 - Annotate our off-chain records with corrections
 - Issue compensating transactions (e.g., refund if wrong amount)
 - Update beneficiary information in our off-chain systems
 - However, we cannot alter the original blockchain transaction record
- **Address Corrections:** If you provide an incorrect wallet address:
 - Transactions already sent cannot be recalled
 - We update your stored address in our system for future transactions
 - We may require re-verification before sending to new address

4. Data Protection by Design and Default

We implement blockchain interactions with privacy in mind:

- **Minimal On-Chain Data:** Only transaction-critical data goes on-chain (wallet address, amount, timestamp)
- **Off-Chain Alternatives:** All personal data stored in controlled, erasable off-chain databases
- **Privacy Coins Option:** Where legally permissible, we may support privacy-enhanced cryptocurrencies
- **Address Rotation:** We encourage (but do not require) users to use different addresses for different transactions

5. Transparency

We provide clear information about blockchain characteristics:

- **User Notice:** Before your first transaction, we inform you that blockchain data is permanent
- **Consent for Blockchain Use:** Your first use of our Services constitutes informed consent to necessary blockchain processing
- **Alternative Options:** Where feasible, we inform you of privacy-enhanced alternatives

6. Controller vs. Processor Distinction

Our Role:

- **Controller:** For the linkage between your identity and wallet addresses stored in our systems
- **Not a Controller:** For the public blockchain network itself (we don't control blockchain infrastructure)
- **Legal Basis:** We process blockchain data based on contract performance (Art. 6(1)(b)) - necessary to provide cryptocurrency services

Blockchain Node Operators:

- Independent entities running blockchain nodes are **not** our processors
- They are independent controllers processing publicly available blockchain data
- We have no control over their processing or their compliance with GDPR

7. Transfer Outside the EEA

Blockchain networks are global and inherently involve international data transfers:

- **Global Distribution:** Blockchain data is automatically replicated to nodes worldwide, including in countries without GDPR adequacy decisions
- **Transfer Safeguard:** The use of pseudonymization (wallet addresses without identity linkage) serves as a safeguard
- **No Alternative:** Global blockchain infrastructure is technically necessary for cryptocurrency services
- **User Awareness:** By using our cryptocurrency services, you acknowledge this inherent global distribution

8. Legal Basis for Blockchain Processing

Our legal basis for processing data on blockchains:

1. **Contract Performance (Art. 6(1)(b)):** Blockchain transactions are technically necessary to provide cryptocurrency on-ramp/off-ramp services you requested
2. **Legal Obligation (Art. 6(1)(c)):** Some jurisdictions require blockchain transaction monitoring for AML compliance
3. **Informed Consent:** For operations beyond strict necessity, we obtain your consent with full explanation of blockchain characteristics

Your Rights Regarding Blockchain Data

You have the right to:

- **✓ Access:** Receive a list of all wallet addresses linked to your identity in our systems
- **✓ Portability:** Receive a machine-readable export of transaction metadata we store about you (off-chain)
- **✓ Erasure of Linkages:** Have us delete all connections between your identity and wallet addresses
- **✓ Object:** Object to blockchain analytics processing beyond legal requirements
- **✓ Information:** Receive detailed information about what blockchain data exists and why

Technical Limitations You Should Understand:

- **✗** We cannot delete wallet addresses or transactions from public blockchains
- **✗** We cannot control what other entities (exchanges, analytics firms) know about your addresses
- **✗** We cannot prevent blockchain data from being replicated globally
- **✗** We cannot edit blockchain transaction records

Blockchain Analytics and Third-Party Access

Third-Party Blockchain Analysis:

- Companies like Chainalysis, Elliptic, and CipherTrace independently analyze public blockchains
- They may identify patterns and cluster addresses without our involvement
- We have no control over their independent processing of public blockchain data
- We use their services for AML compliance, but they are independent controllers

Your Addresses May Be Linked By:

- Other exchanges or services where you've used the same addresses
- Public blockchain explorers (Etherscan, Blockchain.com, etc.)
- Academic researchers analyzing blockchain networks
- Law enforcement using blockchain forensics
- Your own public disclosure (social media, forums, etc.)

Our Responsibility: We are responsible only for the linkages in our own systems, not for linkages made by independent third parties analyzing public blockchain data.

When Blockchain Erasure Obligations Apply

We acknowledge that:

1. **For cryptocurrency wallets you create with us and we control:** We are a data controller and erasure obligations apply fully

2. **For external wallets you connect to our service:** Blockchain data was already public; we are controller only for our internal linkage records
3. **For transaction data on public blockchains:** We implement erasure through delinking; blockchain immutability is a recognized technical constraint

GDPR Recitals and Blockchain

Our approach aligns with:

- **Recital 26:** Pseudonymized data that cannot be attributed to a specific data subject without additional information qualifies for relaxed GDPR obligations
- **Recital 39:** Pseudonymization reduces risks and helps controllers meet data protection obligations
- **Article 11:** If we can no longer identify you (after delinking), we're not obliged to maintain, acquire, or process additional information to comply with GDPR requests

Supervisory Authority Guidance

We follow guidance from:

- European Data Protection Board: Recommendations on data protection by design and by default
- Autoriteit Persoonsgegevens (The Dutch Data Protection Authority, AP)

Future-Proofing

We actively monitor:

- Development of privacy-preserving blockchain technologies (zero-knowledge proofs, private blockchains)
- Regulatory guidance and case law on blockchain and GDPR
- Technical solutions for enhanced on-chain privacy

As technology and guidance evolve, we will update our blockchain data processing practices accordingly.

Questions About Blockchain and Your Rights

For specific questions about blockchain processing and your data protection rights:

- **Email:** dpo@banxa.com
- **Subject:** "Blockchain GDPR Question"
- We will provide detailed, individualized responses within 30 days

Disclaimer

This section represents our good-faith interpretation and implementation of GDPR requirements in the context of blockchain technology. As this is an evolving area of law, we remain open to guidance from supervisory authorities and commit to adjusting our practices as necessary.

