

# BlockWill Analytical Technologies Limited

## PRIVACY POLICY

*Effective Date: January 1, 2026*

*Version 1.0*

### PRIVACY AT A GLANCE

**For BlockWill users, this means that we:**

- DO NOT have access to your private keys or wallet seed phrases
- DO NOT sell your Personal Information to third parties
- DO NOT collect or retain Personal Information unless necessary for our Services and necessary compliances.
- DO store all personal data OFF-CHAIN with only verification hashes on blockchain.
- DO use military-grade encryption to protect your sensitive information
- DO provide you with rights to access, correct, and delete your data
- DO comply with DIFC Data Protection Law No. 5 of 2020

## 1. INTRODUCTION AND SCOPE

### 1.1 About This Privacy Policy

This Privacy Policy ("Policy") describes how BlockWill Analytical Technologies Limited, a company incorporated with Dubai International Financial Centre ("BlockWill," "Company," "we," "us," or "our"), collects, uses, discloses, and protects Personal Information when you use our blockchain-based digital estate planning platform, including our website, mobile applications, Secure Vault, DigiWish, VaultRelay, and related services (collectively, the "Platform" or "Services").

BlockWill is committed to protecting your privacy and ensuring transparency about our data practices. This Policy is designed to comply with the Dubai International Financial Centre Data Protection Law No. 5 of 2020 ("DIFC DP Law"), as amended, and other applicable data protection laws.

### 1.2 Data Controller Information

BlockWill is the data controller responsible for your Personal Information. You can contact us regarding privacy matters at [privacy@blockwill.io](mailto:privacy@blockwill.io).

### 1.3 Scope of This Policy

This Policy applies to all individuals who interact with BlockWill, including:

- Asset Owners who create accounts and use our estate planning Services
- Beneficiaries designated to receive information or assets through VaultRelay

- Executors and Guardians designated to administer estate plans
- Asset Managers appointed to manage accounts on behalf of Asset Owners
- Website visitors and prospective users
- Users accessing BlockWill through Channel Partners (institutions, wealth managers, financial advisors, crypto exchanges etc.)

## **2. INFORMATION WE COLLECT**

### **2.1 Information You Provide Directly**

#### **Account Registration Information:**

- Full legal name, date of birth, nationality, and country of residence
- Email address, phone number, and mailing address
- Government-issued identification documents for identity verification (KYC)
- Proof of address documentation
- Username and password credentials

#### **Estate Planning Information:**

- Asset inventory details (descriptions, locations, values, account numbers etc.)
- Digital asset information (wallet addresses, cryptocurrency holdings, NFT collections etc.)
- Traditional asset information (real estate, financial accounts, personal property etc.)
- Beneficiary designations and contact information
- Executor and Guardian designations and contact information
- DigiWish intentions and succession instructions
- VaultRelay trigger configurations and conditions
- Documents uploaded to Secure Vault

#### **Special Category Data (Sensitive Personal Information):**

With your explicit consent, we may collect:

- Religious beliefs (for Sharia-compliant estate planning and Islamic inheritance distribution)
- Family structure and relationships (for inheritance configurations)
- Biometric data (if enabled for enhanced authentication)

### **2.2 Information About Third Parties**

When you create an estate plan, you may provide us with Personal Information about other individuals, including:

- Beneficiaries: Names, contact information, dates of birth, relationships to you, and allocation details
- Executors: Names, contact information, and authority designations
- Guardians: Names, contact information for minor beneficiary management

- Family Members: Information relevant to inheritance configurations

**Your Responsibility:**

You represent and warrant that you have the necessary authority to provide this information and that you will inform these individuals about our processing of their data. We will notify beneficiaries and other designated individuals of our processing in accordance with the Terms of Use and applicable law.

**2.3 Information Collected Automatically**

**Technical and Usage Information:**

- IP address, device type, operating system, and browser type
- Unique device identifiers
- Login timestamps, session duration, and feature usage patterns
- Pages visited, links clicked, and navigation paths on our website
- Error logs and performance data

**Blockchain Interaction Data:**

- Transaction hashes for verification purposes
- Smart contract interaction records
- On-chain verification timestamps

**Cookies and Similar Technologies:**

We use cookies, pixels, and similar tracking technologies as described in Section 11 of this Policy.

**2.4 Information from Third Parties**

- Identity verification results from KYC service providers
- Information from Channel Partners who refer you to our Services
- Publicly available blockchain data
- Information from internet platforms if you choose to connect accounts

### 3. HOW WE USE YOUR INFORMATION

#### 3.1 Primary Purposes

We process your Personal Information for the following primary purposes:

##### Providing Our Services:

- Creating and managing your BlockWill account
- Operating Secure Vault encrypted storage
- Generating DigiWish estate planning documents
- Configuring and executing VaultRelay transfers
- Facilitating asset inventory management
- Processing beneficiary, executor, and guardian designations

##### Identity Verification and Security:

- Verifying your identity through KYC processes
- Preventing fraud, unauthorized access, and illegal activities
- Complying with anti-money laundering (AML) and counter-terrorism financing (CTF) requirements
- Protecting the security and integrity of our Platform

##### Communication:

- Sending service-related notifications and alerts
- Responding to your inquiries and support requests
- Providing updates about your estate plan status
- Notifying beneficiaries upon VaultRelay activation

#### 3.2 Legal Bases for Processing

Under DIFC Data Protection Law, we process your Personal Information based on the following legal grounds:

Legal Basis	Processing Activities
Contract Performance	Providing our core Services, managing your account, processing transactions, executing VaultRelay transfers
Legal Obligation	KYC/AML compliance, responding to legal requests, tax reporting, regulatory requirements
Legitimate Interests	Platform security, fraud prevention, service improvement, analytics, customer support
Explicit Consent	Processing religious beliefs for Sharia compliance, health data for triggers, marketing communications, optional features
Vital Interests	Emergency situations where necessary to protect life

#### 3.3 Special Category Data Processing

##### Religious Beliefs (Sharia Compliance):

If you elect Sharia-compliant estate planning, we process information about your religious beliefs solely for the purpose of calculating inheritance distribution according to Islamic law (Faraid). This processing is based on your explicit consent, which you may withdraw at any time. Withdrawal of consent will affect our ability to provide Sharia-compliant distribution calculations.

#### **Health Information:**

If you configure incapacity-based triggers for VaultRelay, we may process health-related information solely for trigger verification purposes. This processing requires your explicit consent and is subject to enhanced security measures.

## **4. BLOCKCHAIN DATA AND IMMUTABILITY**

### **IMPORTANT NOTICE REGARDING BLOCKCHAIN TECHNOLOGY**

#### **4.1 How We Use Blockchain Technology**

BlockWill utilizes blockchain technology to provide tamper-proof verification of your estate planning documents and intentions. Our approach separates personal data storage from blockchain verification:

##### **Off-Chain Storage (Deletable):**

- All Personal Information is stored in our encrypted, off-chain databases
- Estate planning documents and Secure Vault contents
- Beneficiary details and contact information
- Account credentials and authentication data
- All data subject to your rights of access, correction, and deletion

##### **On-Chain Storage (Permanent):**

- Cryptographic hashes (digital fingerprints) of documents for verification
- Timestamps proving when documents were created or modified
- Smart contract states for VaultRelay trigger verification
- Verification proofs that do not contain readable personal information

#### **4.2 Blockchain Immutability Disclosure**

ONCE DATA IS RECORDED ON A BLOCKCHAIN, IT BECOMES PART OF A PERMANENT, IMMUTABLE RECORD THAT CANNOT BE DELETED OR MODIFIED. You acknowledge and understand that:

- Blockchain records are permanent and tamper-proof by design
- We cannot delete, modify, or remove data recorded on public blockchains
- On-chain hashes alone cannot be used to identify you without access to our off-chain systems
- If you exercise your right to erasure, we will delete your personal information from our off-chain systems; any remaining on-chain hashes will become meaningless and unlinkable to you

#### **4.3 Wallet Addresses**

Wallet addresses you connect to our Platform are considered pseudonymous personal data. We collect wallet addresses to:

- Enable digital asset inventory management
- Facilitate VaultRelay transfers of digital assets' information

We do not have access to your private keys or seed phrases. You are solely responsible for maintaining the security of your wallet credentials.

## **5. DATA SHARING AND DISCLOSURE**

### **5.1 Categories of Recipients**

We may share your Personal Information with the following categories of recipients:

#### **Service Providers and Processors:**

- Cloud infrastructure providers (data hosting and storage)
- Database service providers
- KYC and identity verification providers
- Payment processors
- Customer support platforms
- Security and fraud prevention services

#### **Designated Recipients Under Your Estate Plan:**

- Beneficiaries (as authorized by you upon VaultRelay activation)
- Executors (as authorized by you to execute triggers for VaultRelay activation)
- Guardians (as authorized by you for minor beneficiary management)
- Asset Managers (as authorized by you to manage your Secure Vault)

#### **Professional Advisors:**

- Legal counsel (for legal compliance and dispute resolution)
- Auditors (for financial and compliance audits)
- Consultants (for service improvement)

#### **Legal and Regulatory Authorities:**

- Government agencies when required by law
- Law enforcement in response to valid legal process
- Regulatory bodies for compliance purposes
- Courts in connection with legal proceedings

#### **Channel Partners:**

If you access BlockWill through a Channel Partner (institutions like banks, insurance companies, wealth managers, financial advisors, crypto exchanges), we may share limited information with that partner as necessary to provide Services and maintain your relationship with them.

### **5.2 We Do Not Sell Your Personal Information**

BlockWill does NOT sell, rent, or trade your Personal Information to third parties for their marketing purposes. We do not participate in data broker arrangements or sell access to our user database.

### **5.3 Third-Party Data Processing Agreements**

All service providers who process Personal Information on our behalf are bound by written data processing agreements that require them to:

- Process data only on our documented instructions
- Maintain confidentiality obligations
- Implement appropriate security measures
- Assist with data subject rights requests
- Delete or return data upon termination of services
- Submit to security audits and inspections

## **6. INTERNATIONAL DATA TRANSFERS**

### **6.1 Global Data Processing**

BlockWill operates globally and may transfer your Personal Information to countries outside the Dubai International Financial Centre. These transfers are necessary to provide our Services and may occur to:

- United States (cloud infrastructure)
- European Union / European Economic Area (cloud infrastructure)
- Other jurisdictions where our service providers operate

### **6.2 Transfer Safeguards**

When transferring Personal Information outside the DIFC, we implement appropriate safeguards as required by DIFC Data Protection Law:

#### **Adequate Jurisdictions:**

Transfers to jurisdictions recognized by the DIFC Commissioner as providing adequate data protection (including EU/EEA member states, UK, Singapore, and California) may proceed without additional safeguards.

#### **Standard Contractual Clauses:**

For transfers to non-adequate jurisdictions, we use DIFC-approved Standard Contractual Clauses that impose contractual obligations on data recipients to protect your information.

#### **Transfer Impact Assessments:**

We conduct documented assessments before international transfers, evaluating whether data subjects will have adequate legal protections and effective remedies in recipient jurisdictions.

### **6.3 Your Consent to International Transfers**

By using our Services, you acknowledge and consent to the transfer of your Personal Information to jurisdictions outside the DIFC as described in this Policy. You have the right to

obtain information about the specific safeguards applied to any transfer by contacting us at [privacy@blockwill.io](mailto:privacy@blockwill.io).

## 7. DATA RETENTION

### 7.1 Retention Periods

We retain your Personal Information for as long as necessary to fulfil the purposes for which it was collected and to comply with legal obligations. Our standard retention periods are:

Data Category	Retention Period	Justification
Active User Account Data	Duration of account + 7 years	Legal/regulatory requirements
Data After Account Termination	7 years from termination	Legal claims, audit requirements
Data After Asset Owner Death	7 years from estate administration completion	Estate administration, beneficiary access
Blockchain-Recorded Data	Permanent (immutable)	Technical impossibility of deletion
KYC/AML Records	7 years minimum	DIFC AML regulations
Transaction Records	7 years	Financial record requirements
Marketing Preferences	Until consent withdrawal + 2 years	Compliance demonstration

### 7.2 Estate Planning Retention Justification

Estate planning requires extended data retention because:

- Estate plans may not be executed for many years or decades after creation
- Beneficiaries may need access to information long after the Asset Owner's death
- Legal disputes regarding estates may arise years after death
- Regulatory requirements mandate retention of financial and legal records
- Proof of testamentary intent may be required for probate proceedings

### 7.3 Data Deletion

When retention periods expire, we securely delete or anonymize your Personal Information. For blockchain-recorded data, we implement “practical erasure” by deleting all off-chain personal information, rendering any on-chain hashes meaningless and unlinkable to you.



## **8. DATA SECURITY**

### **8.1 Security Measures**

We implement comprehensive technical and organizational measures to protect your Personal Information:

#### **Technical Safeguards:**

- AES-256 encryption for data at rest in Secure Vault
- TLS 1.3 encryption for data in transit
- Zero-knowledge architecture where possible
- Multi-factor authentication (MFA) for account access
- Hardware security modules (HSMs) for key management
- Regular security audits and penetration testing
- Intrusion detection and prevention systems
- DDoS protection and web application firewalls

#### **Organizational Safeguards:**

- Role-based access controls with least privilege principles
- Employee background checks and confidentiality agreements
- Regular security awareness training
- Incident response procedures
- Business continuity and disaster recovery plans
- Third-party security assessments of service providers

### **8.2 Security Certifications**

Our infrastructure and service providers maintain industry-recognized security certifications including:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- SOC 2 Type II
- PCI DSS (where applicable for payment processing)

### **8.3 Your Security Responsibilities**

You are responsible for:

- Maintaining the confidentiality of your account credentials
- Using strong, unique passwords
- Enabling multi-factor authentication
- Securing your devices and internet connections
- Protecting your private keys and wallet seed phrases
- Promptly reporting any suspected unauthorized access

## **8.4 Data Breach Response**

In the event of a data breach affecting your Personal Information, we will:

- Investigate and contain the breach promptly
- Notify the DIFC Commissioner of Data Protection as required by law
- Notify affected individuals if the breach poses a high risk to their rights and freedoms
- Document all breaches and remedial actions taken

## **9. YOUR DATA PROTECTION RIGHTS**

### **9.1 Rights Under DIFC Data Protection Law**

Under DIFC Data Protection Law, you have the following rights regarding your Personal Information:

#### **Right of Access:**

You have the right to obtain confirmation of whether we process your Personal Information and to access a copy of that information, along with details about the processing.

#### **Right to Rectification:**

You have the right to request correction of inaccurate Personal Information and completion of incomplete information.

#### **Right to Erasure (“Right to be Forgotten”):**

You have the right to request deletion of your Personal Information when it is no longer necessary for the purposes collected, you withdraw consent, the processing is unlawful, or you validly object to processing. This right is subject to legal retention requirements and blockchain immutability limitations described in Section 4.

#### **Right to Restriction of Processing:**

You have the right to request that we restrict processing of your Personal Information in certain circumstances, such as while we verify accuracy or assess an objection.

#### **Right to Data Portability:**

You have the right to receive your Personal Information in a structured, commonly used, machine-readable format and to transmit that data to another controller.

#### **Right to Object:**

You have the right to object to processing based on legitimate interests or for direct marketing purposes.

#### **Right to Withdraw Consent:**

Where processing is based on consent, you have the right to withdraw consent at any time. Withdrawal does not affect the lawfulness of processing before withdrawal.

#### **Right Not to be Subject to Automated Decision-Making:**

You have the right not to be subject to decisions based solely on automated processing that significantly affect you, unless necessary for contract performance, authorized by law, or based on explicit consent.

## **9.2 How to Exercise Your Rights**

To exercise any of your rights, please contact us at [privacy@blockwill.com](mailto:privacy@blockwill.com)

We will respond to your request within one (1) month of receipt. This period may be extended by two additional months for complex requests, in which case we will inform you of the extension and reasons.

## **9.3 Verification**

To protect your privacy, we may need to verify your identity before fulfilling your request. This may include requesting additional information or documentation.

## **9.4 Right to Lodge a Complaint**

If you believe we have not handled your Personal Information properly, you have the right to lodge a complaint with the DIFC Commissioner of Data Protection:

DIFC Commissioner of Data Protection

Email: [commissioner@dp.difc.ae](mailto:commissioner@dp.difc.ae)

Website: [www.difc.ae/data-protection](http://www.difc.ae/data-protection)

You also have the right to bring a claim directly before the DIFC Courts for compensation for damages arising from breaches of data protection law.

# **10. BENEFICIARY AND THIRD-PARTY DATA**

## **10.1 Information About Beneficiaries**

When you provide Personal Information about beneficiaries, executors, guardians, or other third parties, we process this information based on legitimate interests (fulfilling your estate planning instructions) or your contractual relationship with us.

## **10.2 Notice to Beneficiaries**

We will provide privacy notices to asset managers and executors within one (1) day upon their appointment by you in their respective role. We will provide privacy notices to beneficiaries and guardians within one (1) day upon trigger of your VaultRelay based on your instructions. This notice will include:

- Our identity and contact details
- The purposes of processing their information
- The source of their information (i.e., that you provided it)
- Their data protection rights
- How long we will retain their information

## **10.3 Beneficiary Rights**

Beneficiaries and other designated individuals have the same data protection rights described in Section 9. They may contact us directly to exercise these rights.

## 10.4 Data Processing After Death

Upon verified notification of an Asset Owner's death:

- The deceased's Personal Information ceases to be protected under DIFC data protection law (which applies only to living individuals)
- Designated executors will receive access to estate planning documents as specified in the estate plan
- Beneficiary and family member information (living persons) remains fully protected
- We will handle the deceased's information in accordance with documented preferences and estate administration requirements
- Data will be retained for 7 years following completion of estate administration

## 11. COOKIES AND TRACKING TECHNOLOGIES

### 11.1 Types of Cookies We Use

We use the following categories of cookies and similar technologies:

#### Essential Cookies (Required):

These cookies are necessary for the Platform to function and cannot be disabled. They include authentication cookies, security cookies, and load balancing cookies.

#### Functional Cookies (Optional):

These cookies enable enhanced functionality and personalization, such as remembering your preferences and settings.

### 11.2 Your Cookie Choices

In accordance with DIFC requirements, our default privacy settings collect only minimum necessary data. Upon your first visit, you will be prompted to actively select your cookie preferences. You can change your preferences at any time through:

- Our cookie preference center accessible from any page
- Your browser settings
- Mobile device settings for app-based tracking

### 11.3 Do Not Track

We honor Do Not Track (DNT) signals from browsers. When DNT is enabled, we disable non-essential tracking technologies.

## 12. CHILDREN'S PRIVACY

Our Services are not directed to individuals under the age of 18. We do not knowingly collect Personal Information from children. If you are a parent or guardian and believe your child has provided us with Personal Information, please contact us immediately, and we will delete such information.

Where minor beneficiaries are designated in estate plans, their information is provided by the adult Asset Owner and is processed for estate administration purposes. Guardians are designated to manage beneficiary access for minors.

## **13. CHANGES TO THIS PRIVACY POLICY**

### **13.1 Policy Updates**

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. The “Effective Date” at the top of this Policy indicates when it was last materially revised.

### **13.2 Notification of Changes**

For material changes to this Policy, we will:

- Provide at least thirty (30) days’ advance notice via email
- Display a prominent notice on our Platform
- Update the Effective Date
- Maintain archived versions of previous policies

### **13.3 Continued Use**

By continuing to use our Services after changes take effect, you accept the revised Privacy Policy. If you do not agree with the changes, you should discontinue use of the Platform.

## **14. CONTACT US**

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at [privacy@blockwill.io](mailto:privacy@blockwill.io).

We aim to respond to all privacy-related inquiries within five (5) business days.

## ACKNOWLEDGMENT

By using the BlockWill Platform, you acknowledge that you have read, understood, and agree to the collection, use, and disclosure of your Personal Information as described in this Privacy Policy.

You further acknowledge that:

- You understand our use of blockchain technology and its immutability implications
- You consent to international transfers of your Personal Information as described herein
- You have authority to provide Personal Information about beneficiaries, guardians, executors, asset managers and other third parties
- You understand your data protection rights and how to exercise them

© 2026 BlockWill Analytical Technologies Limited All Rights Reserved.

*BlockWill™, DigiWish™, Secure Vault™, and VaultRelay™  
are trademarks of BlockWill Analytical Technologies Limited*

Version 1.0 | Effective Date: January 1, 2026