

EFFECTIVE DATE: 17 April 2026

This Privacy Policy (this “**Policy**”) applies to the trading platform (including any applicable mobile applications and websites used to access the same) (collectively the “**Platform**”) provided by Bybit Technology Limited (the “**Company**,” “**we**,” “**us**” or “**our**”). It describes how the Company collects, uses, and discloses Personal Information that we obtain from Users of the Platform and any account services provided through the Platform, and how we use and disclose that information. For purposes of this Policy, “**Personal Information**” refers to information supplied by a User from which the identity of such User may be directly or indirectly determined.

We prioritize the security and privacy of your Personal Information. We are committed to ensuring that all Personal Information is processed in accordance with the highest standards of data protection and privacy regulations, and that technical and organizational measures are put in place. Our robust data management practices are designed to safeguard your information and maintain your trust.

It is important that you familiarize yourself with the provisions of this Policy together with Terms and Conditions and any other privacy notices we may provide on specific occasions when we are collecting or processing Personal Information so that you are fully aware of how and why we are using your Personal Information.

By registering for and using the Platform, to the extent permitted under applicable law, you agree that your Personal Information will be handled as described in this Policy and the Terms and Conditions applicable to the Platform (the “**Service Agreement**”); capitalized terms used herein shall have the same meaning as set forth in the Service Agreement.

Lawful basis for processing Personal Information

We process your Personal Information using one of the following legal basis:

- a) **Performance of a contract** means processing your Personal Information where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract;

- b) **Legitimate interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Information for our legitimate interests. We do not use your Personal Information for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us;
- c) **Legal requirement** means processing your Personal Information where it is necessary for compliance with a legal or regulatory obligation that we are subject to;
- d) **Consent** means processing your Personal Information using your written consent.

Note that we may process your Personal Information for more than one lawful ground depending on the specific purpose for which we are using your Personal Information. Please contact us if you need details about the specific legal ground we are relying on to process your Personal Information.

Generally, we do not rely on consent as a legal basis for processing your Personal Information other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

The Information We Collect About You and How We Use Your Information

We collect and process Personal Information about you directly from you when you register to use the Platform or submit such information automatically through your use of the Platform, as well as from third parties to comply with the law or with our regulatory obligations. Such information is used to enforce or apply our Service Agreement and other agreements, to protect the rights, property or safety of the Platform and our Users or others, and to facilitate and ensure the provision of services and products offered by the Platform.

Data minimisation and purpose limitation. We will only collect, use, disclose and otherwise process the minimum amount of Personal Information that is necessary to achieve the specific purposes described in this Policy (or otherwise notified to you at the time of collection). We will not process

Personal Information in a manner that is incompatible with those purposes unless we have identified an additional lawful basis that permits the new purpose.

Please note that if you are acting as an Authorized Individual on behalf of a User and are providing Personal Information for such User, you are responsible for ensuring that you have all required permissions and consents to provide such Personal Information to us for use in connection with the Platform and that our use of such Personal Information you provide to the Platform does not violate any applicable law, rule, regulation or order.

In addition, please be advised that the information you provide will be screened against risk profiles to comply with applicable Anti-Money Laundering rules and internal “Know Your Client” policy.

The followings are the personal information that the Company collects and maintains

Classification	Purposes of Processing Personal Information	Items of Personal information	Retention Period
<i>Know your customer (“KYC”) process</i>	<i>Verify ID’s photo with applicants image.</i>	<i>Biometrics.</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>KYC process</i>	<i>Verify Customer’s ID document’s validity, Client transaction monitoring and analysis in accordance with legal obligations under applicable anti-money laundering and counter-terrorism financing laws.</i>	<i>Passport number, driver’s license number, foreigner registration number.</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>KYC process</i>	<i>PEP (Politically Exposed Person) screening, risk assessment for secure service operation, prevention of misuse, Client transaction monitoring and analysis in accordance with legal obligations under applicable anti-money laundering and counter-terrorism financing laws.</i>	<i>Affiliation with political organisations or other political activities.</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>KYC process</i>	<i>Data obtained during background check, Client transaction monitoring</i>	<i>Criminal records.</i>	<i>For as long as necessary to fulfil</i>

	<i>and analysis in accordance with legal obligations under applicable anti-money laundering and counter-terrorism financing laws.</i>		<i>the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>KYC process</i>	<i>Client due diligence, identification, verification and risk assessment in accordance with Anti-Money Laundering (AML) obligations, Client transaction monitoring and analysis in accordance with legal obligations under applicable anti-money laundering and counter-terrorism financing laws.</i>	<i>Identity documents (e.g., passport) and address verification documents (e.g., utility bills), background check data, (e.g., results from Politically Exposed Persons (PEP) screening ,sanction screening results).</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>Marketing and Promotional Purposes</i>	<i>To send you news and newsletters, special offers, and promotions, to conduct sweepstakes and contests, or to otherwise contact you about products or information we think may interest you.</i>	<i>Name, Surname, Email address, Telephone number, Referral ID</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>Service Provision</i>	<i>Confirmation of intent to register, identification and authentication of users for the provision of membership-based services, and maintenance and management of membership status.</i>	<i>Account data: account number (UID), account creation date, verification safeguards.</i> <i>Contact details: address, email address, phone number.</i> <i>Device data: device type, operating system, unique device identifiers, crash logs, browser type.</i> <i>Log data: IP address, timestamps, login location, user activity.</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>

Service Provision	Processing of financial transactions in the context of crypto exchange and payment card services.	Financial and transactional data: bank account details, credit card data, tax identification number, financial transaction data (e.g., asset details, sender and recipient information).	For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.
Service Provision	Provision of Client support services and handling of Client requests, complaints or inquiries submitted via communication channels.	Name and surname, email address, telephone number, any personal data voluntarily provided by the Client during the support interaction (e.g., information related to the inquiry).	For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.
Service Operation	Client due diligence, identification, verification and risk assessment in accordance with Anti-Money Laundering (AML) obligations, Client transaction monitoring and analysis in accordance with legal obligations under applicable anti-money laundering and counter-terrorism financing laws.	Identification details: full name, date and place of birth, nationality, and photograph. Contact details: residential address, email address, phone number; certificates (e.g. employment, inheritance), nationality / residence). Financial and transactional data: bank account details, credit card data, tax identification number, employment status and income, financial transaction data (e.g., asset details, sender and recipient data).	For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.
Service Operation	Protection of the integrity, confidentiality, and availability of the Company's IT infrastructure, including the detection, prevention, and mitigation of cybersecurity threats and misuse.	Device data: device type, operating system, unique device identifiers, crash logs, browser type.	For as long as necessary to fulfil the relevant purpose, and thereafter as required or

		<i>Log data: IP address, timestamps, login location, user activity.</i>	<i>permitted by applicable law and regulatory obligations.</i>
<i>Service Operation</i>	<i>Fraud prevention and detection, including prevention of fraudulent activities, unauthorized access, and misuse of the Company's services and systems.</i>	<i>Financial and transactional data: bank account details, credit card data, tax identification number, financial transaction data (e.g., asset details, sender and recipient data).</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>Service Operation</i>	<i>To tailor the content and information that we may send or display to you, to offer location customization, and personalized help and instructions, and to otherwise personalize your experiences while using our Platform.</i>	<i>Information that your browser sends whenever you visit the Platform or your mobile application sends when you're using it (Internet Protocol address, the address of the web page you visited before coming to the Platform, your browser type and settings, the date and time of your request, information about your browser configuration and plug-ins, language preferences, and cookie data, information about the device you use for the Platform, including what type of device it is, what operating system you're using, device settings, unique device identifiers, and crash data), Geolocation.</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.</i>
<i>Service Operation</i>	<i>To better understand how Users access and use the Platform, both on an aggregated and individualized basis, in order to improve our Platform and respond to user desires and preferences, and for other research and analytical purposes.</i>	<i>Information that your browser sends whenever you visit the Platform or your mobile application sends when you're using it (Internet Protocol address, the</i>	<i>For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and</i>

		address of the web page you visited before coming to the Platform, your browser type and settings, the date and time of your request, information about your browser configuration and plug-ins, language preferences, and cookie data, information about the device you use for the Platform, including what type of device it is, what operating system you're using, device settings, unique device identifiers, and crash data).	regulatory obligations.
Service Operation	Operation and maintenance of the website and mobile applications	Platform usage data: login history, device type, user preferences and interaction history; Device data: device type, operating system, unique device identifiers, crash logs, browser type; Log data: IP address, timestamps, login location, user activity; Cookie identifiers and analytics data.	For as long as necessary to fulfil the relevant purpose, and thereafter as required or permitted by applicable law and regulatory obligations.

Information We Collect From Third Parties

We may obtain information about you from third parties such as our affiliates, subsidiaries, vendors, analytics service providers, advertising service providers, information search service providers, or publicly available sources as required or permitted by applicable law as set out below:

Maintain legal and regulatory compliance. Processing is necessary to comply with our legal obligations under applicable laws and regulations, including Anti-Money Laundering laws and

regulations. For example, the verification of details concerning sanctions screening and politically exposed persons listings.

Provide services. Our legitimate interest is that you and other Users could access and utilize services and products offered by the Platform with a smooth and personalized experience, as well as be informed about the crypto news or updates. For instance, the aggregation of relevant posts or updates from financial platforms, forums, and social media regarding emerging crypto investment opportunities enables us to curate personalized crypto investment suggestions or alerts for Users based on their preferences and past engagement with the Platform.

These third parties may collect Personal Information on behalf of the Company, or act as separate controllers in accordance with their own privacy policies. Some of these third parties may have obtained your data from publicly accessible sources.

How We Share Your Information

In addition, we, our affiliates, subsidiaries, or third-party service providers may transfer or disclose your Personal Information to:

- comply with any applicable Anti-Money Laundering rules, sanctions or any legal obligation required under legal requirement (e. g. to any Governmental Authority);
- enforce any part of our agreements concluded between you and us or to investigate potential breaches; or
- protect our rights or our property, or those of our other customers. This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

We require all third parties to respect the security of your Personal Information and to treat it in accordance with the law. We do not allow our third-party service providers to use your Personal Information for their own purposes and only permit them to process your Personal Information for specified purposes and in accordance with our instructions.

The specific circumstances under which we transfer or disclose Personal Information to third

parties are set out below.

Affiliates. We may disclose the information we collect from you to our affiliates or subsidiaries solely for the purpose of providing the Platform or related services including subsite services to you; however, if we do so, their use and disclosure of your personally identifiable information will be maintained by such affiliates and subsidiaries in accordance with this Policy.

Service Providers. We may disclose the information we collect from you to third-party vendors, service providers, contractors or agents who perform functions on our behalf, provided such third parties have agreed to only use such information to provide services to us.

Business Transfers. If we are in negotiations with, or are acquired by or merged with another company or entity, if substantially all of our assets are transferred to another company or entity, or as part of a bankruptcy proceeding, we may transfer the information we have collected from you to the other company or entity.

In Response to Legal Process. We also may disclose the information we collect from you in order to comply with the law, a judicial proceeding, court order, or other legal process, such as in response to a subpoena.

To Protect Us and Others. We also may disclose the information we collect from you if we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Service Agreement or this Policy, or as evidence in litigation in which we are involved.

Aggregate and De-Identified Information. We may collect, process, analyze and share aggregate or de-identified information about users with third parties and publicly for product development, marketing, advertising, research or similar purposes.

When sharing your Personal Information with third parties, we will use our best endeavours to ensure that such entities are either subject to this Policy, or follow practices at least as protective as those described in this Policy.

Where we disclose Personal Information to third parties, we will ensure that the disclosure is compatible with the purposes for which the Personal Information was originally collected and disclosed to you. Where a disclosure is for a different purpose, we will only make that disclosure

where it is otherwise duly justified by an additional lawful basis permitted under applicable law (for example, to comply with a legal obligation, to protect vital interests, for public interest reasons, or based on legitimate interests where applicable).

Our Use of Cookies and Other Tracking Mechanisms

We and our third-party service providers use cookies and other tracking mechanisms to track information about your use of our Platform. We may combine this information with other Personal Information we collect from you (and our third-party service providers may do so on our behalf).

Cookies. Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser for record-keeping purposes. Some cookies allow us to make it easier for you to navigate our Platform, while others are used to enable a faster log-in process or to allow us to track your activities at our Platform. There are two types of cookies: session and persistent cookies.

Session Cookies. Session cookies exist only during an online session. They disappear from your computer when you close your browser or turn off your computer. We use session cookies to allow our systems to uniquely identify you during a session or while you are logged into the Platform. This allows us to process your online transactions and requests and verify your identity, after you have logged in, as you move through our Platform.

Persistent Cookies. Persistent cookies remain on your computer after you have closed your browser or turned off your computer. We use persistent cookies to track aggregate and statistical information about user activity.

Please note that our systems do not currently respond to do-not-track signals.

Disabling Cookies. Most web browsers automatically accept cookies, but if you prefer, you can edit your browser options to block them in the future. The general settings on most browsers will tell you how to prevent your computer from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Users of our Platform who disable cookies will not be able to browse certain areas of the Platform.

Third Party Analytics. We use automated devices and applications, such as Google Analytics, to evaluate usage of our Platform. We also may use other analytic means to evaluate our Platform. We use these tools to help us improve our Platform, performance and user experiences. These entities may use cookies and other tracking technologies to perform their services. We do not share your

Personal Information with these third parties.

Third-Party Links

Our Platform may contain links to third-party websites. Any access to and use of such linked websites is not governed by this Policy, but instead is governed by the privacy policies of those third-party websites. We are not responsible for the information practices of such third-party websites.

Security of Your Personal Information

Our security measures. We maintain a robust security program and implement a combination of technical, organisational and physical safeguards designed to protect Personal Information, which include:

- access controls and role-based permissions;
- multi-factor authentication and credential management controls;
- encryption and/or comparable protections for Personal Information in transit and, where appropriate, at rest;
- network security controls;
- logging and monitoring of systems and user activity to help detect, investigate and respond to incidents;
- secure development and change management practices;
- vendor / service-provider security due diligence and contractual controls where third parties process Personal Information on our behalf; and
- incident response and business continuity measures to help restore availability and access following technical incidents.

We have implemented reasonable precautions consistent with applicable laws and regulations to protect the Personal Information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please be aware that despite our efforts, no data security measures can guarantee 100% security. Therefore, all Users (including their Authorized Individuals) of the Platform must comply with the security requirements in the Terms and take the following additional steps to help ensure the security of their Personal Information and the access to their account:

- (a) You should choose a robust user identification, password, and PIN to access your account (“**User**

Credentials”) that nobody else knows or could easily guess. User Credentials must meet the requirements we specify when you establish those User Credentials. You should keep your User Credentials secure and private, and not share your User Credentials with any third party.

(b) You should install anti-virus, anti-spyware, and firewall software in your personal computers and mobile devices;

(c) You should update operating systems, anti-virus, and firewall products with security patches or newer versions on a regular basis;

(d) You should remove file and printer sharing in computers, especially when they are connected to the internet;

(e) You should make regular backups of your critical data;

(f) You should consider the use of encryption technology to protect highly sensitive or confidential information;

(g) You should completely log off and clear your browser cache after finishing each online session with the Platform;

(h) You should not install software or run programs of unknown origin;

(i) You should delete junk or chain emails;

(j) You should not open email attachments from strangers;

(k) You should not disclose personal, financial, or credit card information to little-known or suspect websites;

(l) You should not use a computer or a device that cannot be trusted; and

(m) You should not use public or internet café computers to access online services or perform financial transactions.

You should immediately notify us at support@bybit.com if you become aware of any unauthorized use or access of your Account or User Credentials. We are not responsible for any lost, stolen, or compromised User Credentials or for any activity on your Account via unauthorized activity using your User Credentials.

Rights of access, correction, and deletion

You may exercise the rights described below in relation to your Account and Personal Information by using your account settings (where available) or by contacting us at support@bybit.com (or our Data Protection Officer at dpo@bybit.com).

In particular, you may have the right to:

- Access your Personal Information (including confirmation whether we process it).
- Request correction/rectification of inaccurate, incomplete or out-of-date Personal Information.
- Request deletion/erasure of Personal Information, where applicable.
- Request restriction / blocking of access to your Personal Information (for example, while a correction request is assessed, where you contest accuracy, or where processing is otherwise disputed or must be limited).
- Object / oppose processing of your Personal Information for specific purposes (including, where applicable, direct marketing and certain processing based on legitimate interests), subject to any lawful grounds we may have to continue processing.
- Request for withdrawal of consent to the collection and use of personal information
- Request data portability, meaning you may request that we provide certain Personal Information you have provided to us in a structured, commonly used, machine-readable format, and/or request that we transmit it to a third party where technically feasible and appropriate.

We will respond to your requests within a reasonable period of time, but no later than the time period required by law.

Please note that, to the extent permitted under applicable law, notwithstanding the foregoing, there may be circumstances in which we are unable to accommodate a request to edit, update, access, or delete an account profile or Personal Information. This includes but is not limited to:

- any basis where such request can be denied under applicable law;

- where we need to retain the information to comply with federal, state, or local laws or for accounting or tax purposes;
- where we need to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- where we need to cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law;
- where we need to retain information to exercise or defend legal claims;
- where the information contains legal privilege or proprietary information of another party; or where complying with the request would compromise others' privacy or other legitimate rights.

If we determine that we cannot respond to any request in any particular instance, we will provide you with an explanation of why that determination has been made and a contact point for any further inquiries. To protect your privacy, we will take commercially reasonable steps to verify your identity before responding to any request under this provision, including complying with any applicable legal requirement for verifying your identity. Where applicable, we may also restrict or block access to relevant Personal Information while we verify your identity and/or assess your request.

Overseas Transfer of Information

Please note that the Company collects and processes Personal Information in Seychelles to handle your Personal Information as described in this Policy.

Please note, we may store your Personal Information on servers located in the countries where our main offices are located. We will ensure that security provisions are in place consistent with our obligations to maintain the security of your Personal Information under the laws of your jurisdiction of residence.

The specific details regarding overseas transfer of Personal Information are set out below. If you refuse the overseas transfer, you will not be able to use the service. If you wish to refuse the overseas transfer of your Personal Information, please contact us using the contact details provided in the "Contact Us" section.

Below is a list of overseas transfers of personal information.

Overseas provision of Personal information is subject to the applicable services you will be using

Purpose for Recipient's Use of Personal information	Personal Information Item to be Transferred	Recipient (Entity name, contact info)	Transferred Country	Transfer Time, Method	Retention Period	Contact
<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>Inswitch</i>	<i>USA</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>inswitch_data@inswitch.com</i>
<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>Moon Pay PTE Limited</i>	<i>Singapore</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>dpo@moonpay.com</i>
<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>Xfers Pte LTD</i>	<i>Singapore</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>support@straitstx.com</i>
<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>StraitsX Payment Services Pte Ltd</i>	<i>Singapore</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>support@straitstx.com</i>

<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>Ivy GmbH</i>	<i>Germany</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>privacy@getivy.de</i>
<i>Provision of services</i>	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	<i>STARSPAY EFX FACILITADOR A E SERVIÇOS FINANCEIROS LTDA.</i>	<i>Brazil</i>	<i>On demand via IT systems</i>	<i>Until the purpose is achieved, unless a longer retention period is required by applicable local laws and regulations.</i>	<i>starspay@starspay.com</i>

Overseas Entrustment of Personal information

Purpose for Recipient's Use of Personal information	Personal Information Item to be Transferred	Recipient (Entity name, contact info)	Transferred Country	Transfer Time, Method	Retention Period	Contact
<i>Identification and proof of address documents verifications, including liveliness check</i>	<i>Identification details: full name, date and place of birth, nationality, passport or ID details (e.g., including document number, issuing authority and expiry date), copy of the identification document, and photograph,</i>	<i>Sumsub</i>	<i>United Kingdom</i>	<i>On demand via IT systems</i>	<i>Until cessation of agreement or earlier if requested</i>	<i>privacy@sumsub.com</i>
		<i>Onfido</i>	<i>United Kingdom</i>	<i>On demand via IT systems</i>	<i>Until cessation of agreement or earlier if requested</i>	<i>privacy@entrust.com</i>

	<i>biometrics, IP address; Log data: IP address, timestamps, login location</i>	Advance AI	Singapore	On demand via IT systems	Until cessation of agreement or earlier if requested	dpo@advance.ai
		ZOLOZ	Singapore	On demand via IT systems	Until cessation of agreement or earlier if requested	AntDigital-Global@service.alipay.com
Sanction / PEP and RCA / Terrorist / Negative News screenings	<i>Identification details: full name, passport or ID details (e.g., number, personal code), nationality / residence Verification data: KYC/PEP/sanction screening results), nationality / residence; Criminal Records</i>	LSEG Worldcheck	United Kingdom	On demand via IT systems	Until cessation of agreement or earlier if requested	privacy.enquiries@lseg.com
Transaction monitoring	<i>Transaction data (e.g., asset details, sender, recipient information)</i>	Chainalysis	United States	On demand via IT systems	Until cessation of agreement or earlier if requested	security@chainalysis.com

		<i>Elliptic</i>	<i>Singapore</i>	<i>On demand via IT systems</i>	<i>Until cessation of agreement or earlier if requested</i>	<i>dpo@elliptic.co.</i>
		<i>TRM Labs</i>	<i>United States</i>	<i>On demand via IT systems</i>	<i>Until cessation of agreement or earlier if requested</i>	<i>privacy@trmlabs.com</i>

Retention and Destruction of Personal Information

We retain your Personal Information as long as you maintain an Account on the Platform. We will cease to retain your Personal Information, or remove the means by which the Personal Information can be associated with particular individuals, as soon as it is reasonable to assume that –

- (a) the purpose for which that Personal Information was collected is no longer being served by its retention;
- (b) retention is no longer necessary for legal, accounting or business purposes; and
- (c) consent to the collection and use of the Personal Information has been withdrawn.

Please note that certain laws may require us to retain records of transactions or accounts for a certain period of time.

Once the purpose is achieved, your personal information is moved to a separate database (or a document box in the case of papers) and is destroyed after storage for a certain period depending on data protection reasons under our internal policy and other applicable laws and regulations. The personal information moved to a separate database will not be used for other purposes other than the purpose of retention, unless otherwise provided by laws.

Personal information that has fully served its purpose of collection and use, after expiration of the

retention period of personal information, will be destroyed to an irreversible state. Personal information stored in electronic form is securely deleted by technical means to prevent its recovery or restoration, while written information is shredded or incinerated.

Blockchain Information

You should be aware that due to the inherent transparency of the blockchain networks, transactions that you approve when using the Platform may be publicly accessible. This includes, but is not limited to, your public key address, the public key address of the receiver, the amount of crypto sent or received, and any other data a User has chosen to include in a given transaction.

Transactions and addresses available on blockchain networks may reveal Personal Information about the User's identity, and Personal Information can potentially be correlated now or in the future by any party who chooses to do so, including law enforcement. We encourage you to review how privacy and transparency on blockchain networks works.

Children Under 18

Our Platform is not designed for children under 18. If we discover that a child under 18 has provided us with Personal Information, we will delete such information from our systems.

Data Protection Officer

Where required under applicable data protection law, we designated a Data Protection Officer ("DPO"). The DPO supports oversight of our personal data processing practices, monitors compliance with applicable data protection requirements and acts as a contact point for privacy queries, complaints, and (where applicable) engagement with the Seychelles Information Commission on matters relating to personal data processing.

Name of DPO: Darius Dargis

Contact: dpo@bybit.com

Contact Us

If you have questions about the privacy aspects of our Platform or would like to make a complaint, please contact us via our live chat services, at support@bybit.com, or contact our Data Protection Officer at dpo@bybit.com.

Changes to this Policy

This Policy is current as of the Effective Date set forth above. We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on the Platform. If we make any changes to this Policy that materially affect our practices with regard to the Personal Information we have previously collected from you, we will endeavor to provide you with notice in advance of such change by highlighting the change on our Platform or providing a push notification through the Site (you should make sure your Site settings allow for such push notifications) or sending an email that you have provided in your Account, (for this reason you should make sure to update your account information promptly if it changes).