EFFECTIVE DATE: February 2026

This Privacy Policy (this "**Policy**") applies to the processing of personal data in connection with all services provided by Bybit EU GmbH, legal entity code FN 636180i a company registered at Donau-City-Straße 7, 1220 Vienna, Republic of Austria (the "**Company**," "**we**," "**us**" or "**our**") via trading platform (including any related mobile applications and websites used to access the same) (collectively the "Platform") provided by Bybit Fintech Limited. It describes how the Company collects, uses, and discloses Personal Data processed during provision of its services. This includes, but is not limited to:

- account creation and management;
- identity verification (KYC);
- execution of trades;
- customer support;
- promotional campaigns;
- and any interaction with the Platform ("Services").

This Policy supplements the other Policies and is not intended to override them. Terms used within it shall have the meaning(s) given in the Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)) and the Austrian Data Protection Act (Datenschutzgesetz (DSG)), as applicable.

For purposes of this Policy:

"**Personal Data**" refers to any information relating to an identified or identifiable natural person.

"Processing" refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Controller**" refers to the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Supervisory Authority" refers to the Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Vienna (T +43 1 52 152-0, M dsb@dsb.gv.at).

"**Data Subject**" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly, or indirectly, by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

OUR RELATIONSHIP WITH YOU

We act as the Controller of your personal Data in relation to the Services, ensuring your personal data's safety and complying with applicable regulatory requirements.

As we are responsible for your Personal Data processed providing our Services, we have appointed a Data Protection Officer (DPO) who constantly monitors our compliance with applicable privacy regulations and acts as the contact point for the Supervisory Authority or Data Subjects on issues relating to privacy.

You may contact us in connection with our Services that you are considering or would like to obtain from us, such as cryptocurrency conversion to or from FIAT money.

By registering for and using the Platform, you acknowledge that your Personal Data will be processed as described in this Policy and the Terms and Conditions applicable to the Platform (the "Service Agreement").

If you have any questions or concerns regarding the Processing of your Personal Data, you can contact our Data Protection Officer at dpo@bybit.eu.

LAWFUL BASIS FOR PROCESSING YOUR PERSONAL DATA

We may process your Personal Data on one or more of the following lawful bases, as defined under GDPR:

Performance of a contract: Where the Processing is necessary for the performance of a contract to which you are a party, or to take steps at your request prior to entering into such a contract (Art. 6 (1) lit. b GDPR). This applies, for example, when we provide any of the Services offered through our Platform.

Compliance with legal obligations: Where the Processing is necessary to comply with legal or regulatory obligations to which we are subject, such as anti-money laundering (AML), know-your-customer (KYC), tax reporting, or other applicable compliance requirements (Art. 6 (1) lit. c GDPR).

Legitimate interests: Where the Processing is necessary for the purposes of our legitimate interests (or those of a third party), provided that such interests are not overridden by your fundamental rights and freedoms (Art. 6 (1) lit. f GDPR). Our legitimate interests may include providing and improving our Services, ensuring platform security and tax compliance including internal controls, preventing fraud, and maintaining business operations. We carry out a balancing test to ensure that our interests do not unduly impact your rights. You may contact us for further information regarding this assessment (Legitimate Interest Assessment – LIA).

Consent: In limited cases, we may rely on your (freely given, specific, informed and unambiguous as well as – in certain cases - explicit) consent to process your Personal Data (e.g. for direct marketing or optional features) (Art. 6 (1) lit. (a) GDPR). Where we rely on consent, you are not under any obligation to provide it, and you will not suffer any disadvantage if you choose not to consent or later withdraw it. You may withdraw your consent at any time and without giving any reason, with effect for the future, by contacting us using the contact details provided in this Policy. The withdrawal of consent shall not affect the lawfulness of Processing based on consent before its withdrawal. We ensure that it is as easy to withdraw consent as it is to give it**.**

Please note that we may process your Personal Data based on multiple lawful grounds, depending on the specific purpose for which the data is collected and used. If you would like further information about the legal basis applicable to a specific Processing activity, you may contact us at any time using the details provided in this Policy.

THE PERSONAL DATA WE COLLECT ABOUT YOU AND HOW WE COLLECT IT

We ensure that we only process Personal Data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed, in accordance with the data minimization principle under Art. 5(1)(c) GDPR.
We process Personal Data about you from the following sources:

- Directly from you, for example:
    - when you register to use the Platform or submit such information as a part of the Know-Your-Client (“KYC”) process;
    - when you fill in forms or provide documents on the Platform;
    - when you contact us by email, or through other communication channels;
    - when you submit support requests, participate in dispute resolution, or request assistance;
    - when you physically visit us in our offices or;
    - automatically, through your use of the Platform and our Services.

- From third parties, such as:
    - our partners and affiliates who enable you to use our Services,
    - background screening providers, identity verification services, credit reference agencies, PEP and sanctions screening services,
    - publicly available sources (e.g., official registers or company databases within the EU);

- Data brokers and aggregators, where legally permissible.

In operating our Platform and providing our Services we may process the following Personal Data about you:

a. 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;

b. Contact details: residential address, email address, phone number;

c. Financial and transactional data: source of funds and wealth, bank account details, credit card data (including card number, expiry date and CVC), tax identification number, employment status and income, financial transaction data;

d. Verification data: KYC/PEP/sanction screening results, identity documents, certificates (e.g. employment, inheritance);

e. Employment-related information: employment history, education background, employer reference;

f. Platform usage data: login history, device type, user preferences and interaction history;

g. Device data: device type, operating system, unique device identifiers, crash logs, browser type;

h. Log data: IP address, timestamps, login location, user activity;

i. Account and transaction data: account number (UID), account creation date, account balances, trading history, deposit snapshots, verification safeguards.

Please note: Some of the Personal Data we process is being screened against risk profiles and regulatory watchlists to comply with applicable Anti-Money Laundering laws and internal KYC and Anti-Money Laundering policy (Credit Reference agencies, anti-Fraud agencies, Sanction screening and politically exposed persons (PEP) listings).

PURPOSES FOR WHICH WE PROCESS YOUR PERSONAL DATA

We process your Personal Data as described above for the following purposes and in accordance with the legal bases set out in Art. 6(1) GDPR:

- **To provide and manage access to our Services and your account on the Platform**, including Processing transactions, user authentication, customer service, and technical support (Art. 6(1) lit. b GDPR – performance of a contract).

- **To comply with legal and regulatory obligations**, including anti-money laundering (AML) and counter-terrorism financing laws, tax and accounting obligations, and data retention requirements (e.g. Financial Markets Anti-Money Laundering Act, Federal Fiscal Code, Federal Act Against Unfair Competition; Art. 6(1) lit. c GDPR – compliance with a legal obligation).

- **To ensure the security and integrity of our systems**, including fraud detection, IT security measures, disaster recovery, and audit purposes (Art. 6(1) lit. f GDPR – legitimate interests).

- **To communicate with you about updates, changes, or relevant legal or administrative notices** relating to your account or use of our platform (Art. 6(1) lit. b or c GDPR).

- **To operate and maintain our websites and mobile applications**, including user interface customization, error resolution, and ensuring compatibility across devices and systems (Art. 6(1) lit.f GDPR – legitimate interests).

- **To engage in social media communication and community management**, including responding to user inquiries, moderating content, and maintaining a safe and engaging environment on our official communication channels (Art. 6(1) lit. f GDPR – legitimate interests).

- **To promote our services and products through marketing, user growth initiatives, and**

promotional campaigns, including targeted advertisements, performance tracking, and customer outreach, based on your consent where required (Art. 6(1) lit.a GDPR – consent or Art. 6(1) lit. f GDPR – legitimate interests).

- Where you have provided your consent, for **receiving newsletters, marketing communication or other optional features** (Art. 6(1) lit.a GDPR – consent, which may be withdrawn at any time).

We will only process your Personal Data to the extent necessary for the purposes for which it was collected and in accordance with the principles of data minimization and purpose limitation as defined in the GDPR. If you do not provide us with contractually or legally required Personal Data, we will not be able to provide the services connected with Processing that Personal Data.

HOW WE SHARE YOUR PERSONAL DATA

We may share your Personal Data with the following categories of recipients, in accordance with Art. 13(1) lit. e and 14(1) lit. e GDPR:

- **Group and Affiliates**. We may disclose your Personal Data to our affiliates for the purpose of providing and improving our Services and the Platform.
- **IT Service Providers.** External service providers who support us in hosting, maintaining, and securing our technical systems and infrastructure.
- **Payment and Financial Services Providers.** Providers of payment Processing, banking, and financial infrastructure that facilitate financial transactions and fund movements.
- **Customer Support and Communication Providers.** Providers of communication platforms, call centers, or ticketing systems used for customer interactions and support services.
- **Identity Verification and Compliance Service Providers.** External vendors engaged for identity checks, AML/CTF screening, PEP and sanction list screening, and fraud prevention.
- **Legal Advisors and Auditors.** Professional advisors such as lawyers, auditors, and consultants, where necessary for legal compliance or establishment, exercise or defense of legal claims.
- **Supervisory and Public Authorities.** Governmental or regulatory bodies and law enforcement agencies, where required by applicable law or upon lawful request.
- **Potential Acquirers or Investors.** In the context of corporate transactions such as mergers, acquisitions, or asset transfers, subject to confidentiality obligations.
- **Cloud and Data Storage Providers.** Providers of cloud services and secure data storage.
- **External Tax Advisors.** For the purposes of fulfilling tax compliance obligations and internal controls, we may share your personal data with external tax advisors.
- **Transactional Counterparties.** Where necessary for the performance of our services – in particular for the execution, facilitation or settlement of transactions - we may disclose limited Personal Data (such as wallet addresses, transaction identifiers, or order references) to other users or transactional counterparties involved in the respective transaction. Such disclosure is strictly limited to the minimum personal data necessary to enable the transaction and to comply with applicable legal or contractual obligations.

Wherever we engage these recipients to process Personal Data on our behalf, we do so on the basis of a data processing agreement in accordance with Art. 28 GDPR. These processors are contractually bound to act solely on our documented instructions, to implement appropriate technical and organizational measures to ensure the security and confidentiality of your Personal Data, and not to disclose your data to third parties without our authorization or unless required to do so by law.

However, not all recipients qualify as processors. In certain constellations, they may process Personal Data for their own purposes and under their own responsibility, thereby acting as independent controllers within the meaning of Art. 4(7) GDPR. This may include, for example, financial service providers (e.g., fiat on-ramp providers) who are required under applicable financial or anti-money laundering laws to retain certain data for their own compliance purposes. In such cases, data transfers are based on the respective legal basis

under Art. 6 GDPR and no data processing agreement under Art. 28 GDPR is required.

In specific scenarios, data may also be processed under a joint controllership arrangement within the meaning of Art. 26 GDPR, where two or more parties jointly determine the purposes and means of processing. In such cases, we enter into a joint controller agreement that transparently sets out the respective responsibilities of the parties, in particular with regard to the exercise of data subject rights and compliance with information obligations under Art. 13 and 14 GDPR. The essence of such an arrangement is made available to data subjects upon request.

Disclosures to public authorities, courts, and regulators are made solely on the basis of a legal obligation pursuant to Art. 6(1) lit. c GDPR, and such entities act as independent controllers. Similarly, in the event of corporate transactions (e.g., mergers or acquisitions), potential acquirers may act as separate controllers depending on the context of the Processing.

Where we engage recipients outside the European Economic Area (EEA), your Personal Data may be transferred to and processed in such third countries. These countries may not offer the same level of data protection as that guaranteed within the EEA. In such cases, we will ensure that appropriate safeguards are implemented in accordance with Chapter V of the GDPR, in particular:

- by relying on an adequacy decision issued by the European Commission (Art. 45 GDPR), or
- in the absence of an adequacy decision, by concluding Standard Contractual Clauses (SCCs) adopted by the European Commission (Art. 46(2)(c) GDPR), or
- by implementing other appropriate safeguards in accordance with Art. 46 GDPR, if applicable.

Your Personal Data is transferred to Bybit Technology Limited, located in the Seychelles, as part of our corporate group structure. Furthermore, our systems are operated using Amazon Web Services (AWS) cloud infrastructure, with data storage and computing resources located in Singapore, which also constitutes a transfer of Personal Data to a third country.

These transfers are carried out in accordance with Art. 46(2) lit. c GDPR, based on the European Commission's Standard Contractual Clauses (SCCs). In line with the CJEU ruling in Case C-311/18 ("Schrems II"), we conduct Transfer Impact Assessments (TIAs) to evaluate the legal environment in recipient countries and ensure an essentially equivalent level of protection for your Personal Data. Where necessary, we implement supplementary measures (such as encryption and strict access controls) to complement the SCCs and address potential risks arising from local laws that may conflict with EU data protection principles.

You may request further information or a copy of the relevant safeguards in place by contacting our Data Protection Officer dpo@bybit.eu.

SECURITY OF YOUR PERSONAL DATA

We take the security of your Personal Data seriously. In accordance with Art: 32 GDPR, we implement appropriate technical and organisational measures (TOMs) to ensure a level of security appropriate to the risk, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage of your Personal Data.

These measures include, but are not limited to, access controls, encryption, regular security assessments, and secure software development practices. Our security controls are reviewed and updated regularly in line with industry best practices and technological developments.

To further enhance the security of your account and Personal Data, we strongly encourage you to adhere to the following security practices:

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.eu if you become aware of any unauthorized use or access of your account or User Credentials. While we implement appropriate technical and organisational measures to protect your Personal Data and User Credentials in accordance with Article 32 GDPR, you are responsible for maintaining the confidentiality and security of your login credentials. We cannot be held liable for any unauthorised access or misuse of your account resulting from your failure to adequately protect your login credentials, unless such access results from our own failure to implement appropriate security measures.

YOUR PRIVACY RIGHTS

Pursuant to Art. 13 and 14 GDPR you have the following rights in relation to your Personal Data, subject to the conditions and exceptions set out in the GDPR:

- **Right of Access** (Art. 15 GDPR): You have the right to obtain confirmation as to whether or not Personal Data concerning you is being processed, and, where that is the case, to access such Personal Data, including (but not limited to) information on the purposes of Processing, the categories of Personal Data concerned, and the recipients or categories of recipients.

- **Right to Rectification** (Art. 16 GDPR): You have the right to request the correction of inaccurate Personal Data concerning you and, taking into account the purposes of the Processing, the completion of incomplete Personal Data.

- **Right to Erasure ("Right to be Forgotten")** (Art. 17 GDPR): You have the right to request the deletion of your Personal Data in certain circumstances, for example, if the data is no longer necessary for the purposes for which it was collected, or if you have withdrawn your consent (where applicable) and there is no other legal ground for Processing.

- **Right to Restriction of Processing** (Art. 18 GDPR): You may request the restriction of Processing where one of the conditions under Art. 18 GDPR applies, such as when the accuracy of the Personal Data is contested or the Processing is unlawful but you oppose the erasure of the data.

- **Right to Data Portability** (Art. 20 GDPR): Where Processing is based on consent or on a contract and is carried out by automated means, you have the right to receive the Personal Data you provided to us in a structured, commonly used and machine-readable format, and to transmit those data to another controller.

- **Right to Object** (Art. 21 GDPR): Where the Processing is based on our overriding legitimate

interests (Art. 6(1) lit. f GDPR), you have the right to object to such Processing on grounds relating to your particular situation. We shall no longer process the Personal Data unless we demonstrate compelling legitimate grounds for the Processing.

- **Right to Withdraw Consent**: Where Processing is based on consent (Art. 6(1) lit. a or Art. 9(2) lit. GDPR), you have the right to withdraw your consent at any time. The withdrawal of consent does not affect the lawfulness of Processing based on consent before its withdrawal.

- **Right not to be subject to Automated Decision-Making** (Art. 22 GDPR): You have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, except in cases permitted by the GDPR.

- **Right to Lodge a Complaint** (Art. 77 GDPR): You have the right to lodge a complaint with Supervisory Authority, the DSB, located at Barichgasse 40–42, 1030 Vienna, Austria (https://www.dsb.gv.at).

- **Right to Compensation** (Art. 82 GDPR): If you have suffered material or non-material damage as a result of a breach of the GDPR, you have the right to receive compensation from the controller or processor responsible for the damage. You may bring a claim for compensation before the competent court in the Member State in which you reside. This right is without prejudice to any other administrative or judicial remedies available to you.

You may exercise these rights free of charge. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive nature, we may either:

- Charge a reasonable fee based on administrative costs; or
- Refuse to act on the request.

Where a fee is charged, it will be based on the administrative costs of fulfilling your request.

We will respond to your requests without undue delay, and in any case within one month of receipt of the request, in accordance with Art. 12(3) GDPR. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. In such cases, you will be informed of any such extension and the reasons for the delay.

If we are unable to act on your request, we will inform you without delay, and in any case within one month of receipt of the request, and provide reasons for not taking action.

Where we have reasonable doubts concerning the identity of the individual making the request, we may request the provision of additional information necessary to confirm your identity, in accordance with Art. 12(6) GDPR. This helps ensure that your Personal Data is not disclosed to anyone who is not entitled to receive it.Please note that notwithstanding the foregoing, there may be circumstances in which we are unable to accommodate your request. These include, but are not limited to, the following:

- **Retention of Information for Legal Compliance**: We may need to retain your Personal Data to comply with laws, or for accounting or tax purposes. For example, Personal Data relevant to Know Your Customer (KYC) or transactions may be subject to Anti-Money Laundering (AML) laws, which require the retention of certain Personal Data, preventing its deletion (e.g. Section 21 Financial Markets Anti-Money Laundering Act, Section 132(1) Federal Fiscal Code, Sections 190, 212 Business Code);

- **Compliance with Legal Inquiries or Subpoenas**: We may need to retain or disclose your Personal Data to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by authorities. If we receive a judicial subpoena concerning your Personal Data, we are obliged to follow such legal requests.

- **Cooperation with Law Enforcement**: We may need to retain or disclose your Personal Data to cooperate with law enforcement agencies regarding conduct or activities that may violate applicable laws. This includes complying with lawful requests from local law enforcement agencies for Personal

Data.

- **Retention of Data for Legal Claims**: We may need to retain your Personal Data to establish, exercise, or defend legal claims. For example, Personal Data may be required to defend our legal interests in court or other proceedings. This applies only in cases where a relevant procedure is already pending or can be concretely anticipated. A refusal to fulfill your request due to hypothetical proceedings cannot be considered.

- **Legal Privilege or Proprietary Information**: We may need to retain certain documents if it contains legal privilege or proprietary information protected by law. In such cases, fulfilling your request may compromise legal rights or privileged information. In such a case, the request will only be fulfilled to the extent that it is technically possible for us to comply, without impairing legal privilege or proprietary information protected by law.

If you have any concerns about our use of your personal information, you can make a complaint to us at dpo@bybit.eu.

DATA PROTECTION OF USING DIGITAL ASSETS AND BLOCKCHAINS

When using our Services involving digital assets, certain Personal Data may be processed via public blockchain networks. Public blockchains are decentralized ledgers that immutably record transactions across distributed networks. Even though public keys or wallet addresses may not directly identify a person, they can still qualify as personal data under the GDPR, particularly when combined with additional information.

In line with Art. 5(1)(c) GDPR, we apply the principle of data minimisation and seek to limit the recording of Personal Data on blockchains to what is strictly necessary. Where possible, we store additional identifying data off-chain and only write pseudonymous identifiers (e.g. public keys) on-chain.

Please note that blockchain networks are typically not under our control. In public blockchains, there is no hierarchical relationship between participants. Therefore, parties who interact with blockchain data – including miners and node operators – act independently and qualify as separate Controllers under GDPR.

Due to the immutable nature of public blockchains, the erasure or modification of personal data stored on-chain may not be technically feasible. Consequently, some data subject rights (such as rectification or erasure under Art.16 and 17 GDPR) may be limited in practice when it comes to data written to the blockchain. We will always inform you in advance when blockchain-based processing is involved and explain any limitations that may arise.

In cases where blockchain-based transactions result in the international transfer of personal data, such transfers are legitimised under Art. 49(1) lit. b or lit. c GDPR where necessary for the performance of a contract.

RETENTION

We retain your Personal Data only for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements. In particular:

- Personal Data processed for the performance of a contract (Art. 6(1) lit. b GDPR) is generally retained for the duration of the contractual relationship and until the expiry of applicable limitation periods (typically three years under Austrian civil law, Section 1486 General Civil Code), unless longer retention is necessary due to specific circumstances (e.g., ongoing legal disputes). Where the extended limitation period of 30 years under Section 1487 General Civil Code is applicable, Personal Data may be retained for up to 15 years based on practical experience with the enforcement of claims.

- Personal Data for tax or accounting obligations may be stored for a minimum of seven years in accordance with Section 132 Federal Fiscal Code and Section 212 Business Code after the end of

the relevant calendar year.

- Personal Data collected based on your consent (Art. 6(1) lit. a GDPR) will be retained until such consent is withdrawn or the data is no longer required for the purposes for which it was collected. Any further Processing beyond the original purpose will only take place where required by legal obligations - such as the aforementioned tax retention duties or statutory limitation periods (e.g., Section 1486, 1487 General Civil Code).

- Where we are required to retain Personal Data in order to comply with legal obligations or to establish, exercise, or defend legal claims, we may retain such data beyond the standard retention periods where necessary. One relevant example is KYC data, which must be retained for 10 years following the termination of the business relationship, in accordance with anti-money laundering and counter-terrorism financing regulations (in particular, the Financial Markets Anti-Money Laundering Act).

Once the respective retention period has expired, and there is no further legitimate purpose for continued storage, the data will be securely deleted or anonymised in accordance with applicable data protection laws.

AUTOMATED DECISION-MAKING AND PROFILING

In certain instances, we use your personal data for automated decision-making, including profiling, within the meaning of Article 22 GDPR. This may occur in particular to determine whether we can onboard you as a customer.

Such automated decision-making is used only where it is necessary for entering into or performing a contract with you (Art. 22(2)(a) GDPR). These automated systems apply rule-based checks to verify your identity and to assess whether the information provided meets mandatory AML/KYC requirements. Depending on the outcome, your onboarding application may be accepted, declined, or require additional review. The logic involved consists of automated verification and risk-based analysis designed to detect inconsistencies or potential compliance issues. The intended effect for you is that a decision on your onboarding can be made efficiently and in accordance with statutory obligations.

Where a decision is based solely on automated processing and produces legal or similarly significant effects, you have the right (i) to obtain human intervention, (ii) to express your point of view, and (iii) to contest the decision. To exercise these rights, please contact our Customer Support team at support@bybit.eu.

CHILDREN UNDER 14

Our Services are not intended for children under the age of 14. Where we offer information society services directly to a child and rely on consent under Art 6(1) lit. a GDPR as the legal basis for Processing Personal Data, such consent is only valid if the child is at least 14 years old in accordance with Section 4(4) DSG.

If the child is younger than 14, the Processing of their Personal Data is only lawful if and to the extent that consent is given or authorised by the holder of parental responsibility.

If we become aware that we have collected Personal Data from a child under the age of 14 without valid consent, we will delete such data without undue delay, unless we are legally required to retain it.

CONTACT US

If you have any questions about this Privacy Policy or how we process your Personal Data, or if you would like to exercise your rights under Art. 15 to 22 GDPR (e.g. access, rectification, erasure, restriction, objection, data portability), you can contact us at: dpo@bybit.eu

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. For this reason you should make sure to update your account information promptly if it changes.