ZNFTMarket (ZNFT)
PRIVACY and COOKIES POLICY

Protecting your privacy is very important to us. Please review our Privacy Statement in order to better understand our commitment to maintaining your privacy, as well as our use and disclosure of your information.

SCOPE AND UPDATES TO THIS PRIVACY POLICY

This Privacy Policy applies to personal information processed by us, including on our websites, mobile applications, and other online or offline offerings. To make this Privacy Policy easier to read, our websites, mobile applications, and other offerings are collectively called the "Services." For information on our processing of Non-public Information that is subject to Gramm-Leach-Bliley Act ("GLBA"), please see Annex A – GLBA Privacy Notice. Changes to our Privacy Policy. We may revise this Privacy Policy from time to time in our sole discretion. If there are any material changes to this Privacy Policy, we will notify you as required by applicable law. You understand and agree that you will be deemed to have accepted the updated Privacy Policy if you continue to use our Services after the new Privacy Policy takes effect.

LANGUAGES AND TRANSLATION OF AGREEMENT

We will communicate with you in English only.

This user agreement is concluded in English only. Any translation of this user agreement is provided solely for your convenience and is not intended to modify the terms of this user agreement. In the event of a conflict between the English version of this user agreement and a version in a language other than English, the English version shall be the definitive version.

YOUR USE OF INFORMATION; DATA PROTECTION LAWS

If you receive information about another ZNFT customer, you must keep the information confidential and only use it in connection with the ZNFT services. You may not disclose or distribute any information about ZNFT users to a third party or use the information for marketing purposes unless you receive that user's express consent to do so. You may not send unsolicited emails to a ZNFT customer or use the ZNFT services to collect payments for sending, or assist in sending, unsolicited emails to third parties.

To the extent that you (as a seller) process any personal data about a ZNFT customer pursuant to this user agreement, you agree to comply with the requirements of any applicable privacy and data protection laws. You have your own, independently determined privacy policy, notices and procedures for any such personal data that

you hold as a data controller, including a record of your activities related to processing of personal data under this user agreement.

PERSONAL INFORMATION WE COLLECT

We get information about you in a range of ways.

- Information You Give Us. Information we collect from you may include:
- Identity information, such as your first name, last name, username or similar identifier, title, date of birth and gender;
- Contact information, such as your postal address, email address and telephone number;
- Profile information, such as your username and password, interests, preferences, feedback and survey responses;
- Feedback and correspondence, such as information you provide in your responses to surveys, when you participate in market research activities, report a problem with Service, receive customer support or otherwise correspond with us;
- Financial information, such as your credit card or other payment card details;
- Transaction information, such details about purchases you make through the Service and billing details;
- Usage information, such as information about how you use the Service and interact with us;
- Marketing information, such as your preferences for receiving marketing communications and details about how you engage with them;
- Financial information, such as bank account number and bank routing number; financial assets holdings; and
- Technical information, such as your wallet address, application programming interface (API)-key and network information regarding transactions.
- Biometric verification including government ID picture upload when required.

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others' rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

The privacy and data protection laws that may apply include any associated regulations, regulatory requirements and codes of practice applicable to the provision of the services described in this user agreement. If you process personal data from Europe pursuant to this user agreement, we must comply with the EU Directive 95/46 EC or the General Data Protection Regulation (EU) 2016/679 (GDPR).

In complying with such laws, we will:

- implement and maintain all appropriate security measures for the processing of personal data;
- maintain a record of all processing activities carried out under this user agreement; and
- not knowingly do anything or permit anything to be done which might lead to a breach of any privacy data protection laws by ZNFT.

The EU General Data Protection Regulation (GDPR), which governs how personal data of individuals in the EU may be processed and transferred, went into effect on May 25, 2018. GDPR is a comprehensive privacy legislation that applies across sectors and to companies of all sizes. It replaces the Data Protection Directive 1995/46. The overall objectives of the measures are the same – laying down the rules for the protection of personal data and for the movement of data.

GDPR is broad in scope and uses broad definitions. "Personal data" is any information that relates to an identified or identifiable living individual (data subject) such as a name, email address, tax ID number, online identifier, etc. "Processing" data includes actions such as collecting, recording, storing and transferring data.

A company that is not established in the Union may have to comply with the Regulation when processing personal data of EU and EEA residents (EEA countries are Norway, Lichtenstein and Switzerland):
a) If the company offers goods or services to data subjects in the EU; or,
b) If the company is monitoring data subjects' behavior taking place within the EU.

The mere accessibility of a company's website in the EU is insufficient to subject a company to GDPR, but other evidence of the intent to offer goods or services in the EU would be relevant.

As a general rule, companies that are not established in the EU but that are subject to GDPR must designate in writing an EU representative for purposes of GDPR compliance. There is an exception to this requirement for small scale, occasional processing of non-sensitive data.

Fines in case of non-compliance can reach up to 4% of the annual worldwide revenue or 20 million euros – whichever is higher. Companies of all sizes and sectors should consider GDPR as part of their overall compliance effort with

assistance of legal counsel.

The European Commission and Data Protection Authorities are releasing official guidelines to help companies with their compliance process. These documents relate, for instance, to the role of the data protection officer, personal data breach notification, data protection impact assessment.

UK CORPORATE CUSTOMERS

When we refer to "PSD2" in this section we mean the Second EU Payment Services Directive ((EU)2015/2366).

We consider you to be a "Corporate Customer" if, on the date you entered into this user agreement, you are not:

- a consumer, (being an individual acting for purposes other than a trade, business or profession); and
- a micro-enterprise (being an enterprise which employs fewer than 10 persons and has an annual balance sheet that does not exceed 2 million EUR); and
- a UK registered charity with an annual income of less than 1 million GBP.

We may disapply certain provisions of PSD2 for your use of our service if you are a Corporate Customer.

If you are a Corporate Customer:

- you are not entitled to a refund for billing agreement payments;
- where you identify a problem you have up to 60 days from the date on which the problem happened to notify us about it, after which time we have no obligation to investigate and refund you;
- you will only be entitled to lodge a claim through the UK Financial Ombudsman Service where you fulfil the UK Financial Ombudsman Service's claimant criteria from time to time;
- we are not obliged to comply with the information requirements set out in Title III of PSD2 and their equivalents in any implementation of PSD2 in member states of the European Economic Area that may apply to you ("PSD2 transpositions"); and
- articles 72 and 89 of PSD2 and equivalent provisions in PSD2 transpositions do not apply to your use of our service, meaning that, even where we may say so otherwise in this user agreement, we are not liable to you for the losses or damage you may suffer under those articles and provisions.

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the

CCPA regulations provide guidance on how to implement the law. This law secures privacy rights for California consumers, including:

The right to know about the personal information a business collects about them and how it is used and shared;

- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
- Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.
- If you are a California resident, you may ask businesses to disclose what personal information they have about you and what they do with that information, to delete your personal information and not to sell your personal information. You also have the right to be notified, before or at the point businesses collect your personal information, of the types of personal information they are collecting and what they may do with that information. Generally, businesses cannot discriminate against you for exercising your rights under the CCPA. Businesses cannot make you waive these rights, and any contract provision that says you waive these rights is unenforceable.
- By using the Services, you accept the terms of this Policy and our Terms of Use, and consent to our collection, use, disclosure, and retention of your information as described in this Policy. If you have not done so already, please also review our terms of use. The terms of use contain provisions that limit our liability to you and require you to resolve any dispute with us on an individual basis and not as part of any class or representative action. IF YOU DO NOT AGREE WITH ANY PART OF THIS PRIVACY POLICY OR OUR TERMS OF USE, THEN PLEASE DO NOT USE ANY OF THE SERVICES.

COMPLETE AGREEMENT AND THIRD PARTY RIGHTS

This user agreement sets forth the entire understanding between you and us with respect to our service.

If any provision of this user agreement is held to be invalid or unenforceable, such provision shall be struck out and the remaining provisions shall be enforced.

A person who is not a party to this user agreement has no rights under the Contracts (Rights of Third Parties) Act 1999 to rely upon or enforce any term of this user agreement (except for the third parties falling under the definition of “ZERO

WALLET" in the **Indemnification and Limitation of Liability** section above, in respect of their rights as specified in this user agreement) but this does not affect any right or remedy of third parties which exists or is available apart from that act.

ZNFT LOGIN METHOD

We may allow you to authenticate with ZNFT when you log into certain external websites or mobile apps. If we do so, we may share your login status with any third party enabling you to log in in this way, as well as the personal and other wallet information that you consent to being shared so that the third party can recognize you. ZNFT will not give the third party access to your wallet and will only make payments from your wallet to that third party with your specific authorization and instruction.

If you enable visitors to authenticate with ZNFT when they log into your website, app, or your customer wallets, you must agree to any specific terms applicable when this functionality is made available to you and comply with any specifications in any integration manual or guideline. We do not guarantee or otherwise represent the identity of any user of this login method. We will not share with you the personal and other wallet information of the user (including login status) held by ZNFT unless the user has consented to our disclosure of that information to you.

RETENTION OF PERSONAL INFORMATION

We store the personal information we collect as described in this Privacy Policy for as long as you use our Services, or as necessary to fulfill the purpose(s) for which it was collected, provide our Services, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce our agreements, and comply with applicable laws. Please note that due to technical restrictions inherent in the blockchain, deletion of some of your personal information may be difficult or impossible.

YOUR PRIVACY CHOICES AND RIGHTS

Your Privacy Choices. The privacy choices you may have about your personal information are determined by applicable law and are described below.

- Email Communications. If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt out of receiving future emails. Note that you will continue to receive transaction-related emails regarding products or Services you have requested. We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding our Services or updates

to our Terms or this Privacy Policy).

- Text Messages. If you receive an unwanted text message from us, you may opt out of receiving future text messages from us by following the instructions in the text message you have received from us or by otherwise contacting us as set forth in "Contact Us"" below.
- Mobile Devices. We may send you push notifications through our mobile application. You may opt out from receiving these push notifications by changing the settings on your mobile device. With your consent, we may also collect precise location-based information via our mobile application. You may opt out of this collection by changing the settings on your mobile device.
- Phone Calls. If you receive an unwanted phone call from us, you may opt out of receiving future phone calls from us by following the instructions which may be available on the call or by otherwise contacting us as set forth in "Contact Us" below.
- "Do Not Track." Do Not Track ("DNT") is a privacy preference that users can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.
- Cookies and Personalized Advertising. You may stop or restrict the placement of Technologies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for Android, iOS, and others.

The online advertising industry also provides websites from which you may opt out of receiving targeted ads from data partners and other advertising partners that participate in self-regulatory programs. You can access these and learn more about targeted advertising and consumer choice and privacy by visiting the Network Advertising Initiative, the Digital Advertising Alliance, the European Digital Advertising Alliance, and the Digital Advertising Alliance of Canada.

Please note you must separately opt out in each browser and on each device.

Your Privacy Rights. In accordance with applicable law, you may have the right to:

- Access to and Portability of Your Personal Information, including:
    - confirming whether we are processing your personal information;
    - obtaining access to or a copy of your personal information;
    - (where applicable in certain jurisdictions) receiving information regarding public and private entities with which we may have

shared your personal data; and
    - receiving an electronic copy of personal information that you have provided to us, or asking us to send that information to another company in a structured, commonly used, and machine readable format (also known as the "right of data portability");
- Request Correction of your personal information where it is inaccurate or incomplete. In some cases, we may provide self-service tools that enable you to update your personal information;
- Request Deletion of your personal information;
- Request Restriction of or Object to our processing of your personal information;
- Right to object to an automated decision that significantly affects you; and
- Withdraw your Consent to our processing of your personal information. Please note that your withdrawal will only take effect for future processing and will not affect the lawfulness of processing before the withdrawal.

If you would like to exercise any of these rights, please contact us as set forth in "Compliance@iATMGroup.com" below. We will process such requests in accordance with applicable laws. Please note that technical restrictions inherent in the blockchain may make certain requests difficult or impossible (e.g., deletion).

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others' rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

SECURITY OF YOUR INFORMATION

We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy. Unfortunately, no system is 100% secure, and we cannot ensure or warrant the security of any information you provide to us. To the fullest extent permitted by applicable law, we do not accept liability for unauthorized access, use, disclosure, or loss of personal information.
By using our Services or providing personal information to us, you agree that we may communicate with you electronically regarding security, privacy, and administrative issues relating to your use of our Services. If we learn of a security system's breach, we may attempt to notify you electronically by posting a notice on our Services, by mail, or by sending an email to you.

INTERNATIONAL DATA TRANSFERS

All information processed by us may be transferred, processed, and stored anywhere in the world, including, but not limited to, the United States or other countries, which may have data protection laws that are different from the laws where you live. We endeavor to safeguard your information consistent with the requirements of applicable laws.

If we transfer personal information which originates in the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable data protection laws, one of the safeguards we may use to support such transfer is the EU Standard Contractual Clauses.
For more information about the safeguards we use for international transfers of your personal information, please contact us as set forth below.

YOUR PRIVACY CHOICES AND RIGHTS

Your Privacy Choices. The privacy choices you may have about your personal information are determined by applicable law and are described below.

- Email Communications. If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt out of receiving future emails. Note that you will continue to receive transaction-related emails regarding products or Services you have requested. We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding our Services or updates to our Terms or this Privacy Policy).
- Text Messages. If you receive an unwanted text message from us, you may opt out of receiving future text messages from us by following the instructions in the text message you have received from us or by otherwise contacting us as set forth in "Contact Us"" below.
- Mobile Devices. We may send you push notifications through our mobile application. You may opt out from receiving these push notifications by changing the settings on your mobile device. With your consent, we may also collect precise location-based information via our mobile application. You may opt out of this collection by changing the settings on your mobile device.
- Phone Calls. If you receive an unwanted phone call from us, you may opt out of receiving future phone calls from us by following the instructions which may be available on the call or by otherwise contacting us as set forth in "Contact Us" below.

- "Do Not Track." Do Not Track ("DNT") is a privacy preference that users

can set in certain web browsers. Please note that we do not respond to or honor DNT signals or similar mechanisms transmitted by web browsers.

- Cookies and Personalized Advertising. You may stop or restrict the placement of Technologies on your device or remove them by adjusting your preferences as your browser or device permits. However, if you adjust your preferences, our Services may not work properly. Please note that cookie-based opt-outs are not effective on mobile applications. However, you may opt-out of personalized advertisements on some mobile applications by following the instructions for Android, iOS, and others.

The online advertising industry also provides websites from which you may opt out of receiving targeted ads from data partners and other advertising partners that participate in self-regulatory programs. You can access these and learn more about targeted advertising and consumer choice and privacy by visiting the Network Advertising Initiative, the Digital Advertising Alliance, the European Digital Advertising Alliance, and the Digital Advertising Alliance of Canada.

Please note you must separately opt out in each browser and on each device.

Your Privacy Rights. In accordance with applicable law, you may have the right to:

- Access to and Portability of Your Personal Information, including:
    - confirming whether we are processing your personal information;
    - obtaining access to or a copy of your personal information;
    - (where applicable in certain jurisdictions) receiving information regarding public and private entities with which we may have shared your personal data; and
    - receiving an electronic copy of personal information that you have provided to us, or asking us to send that information to another company in a structured, commonly used, and machine readable format (also known as the “right of data portability”);
- Request Correction of your personal information where it is inaccurate or incomplete. In some cases, we may provide self-service tools that enable you to update your personal information;
- Request Deletion of your personal information;
- Request Restriction of or Object to our processing of your personal information;
- Right to object to an automated decision that significantly affects you; and
- Withdraw your Consent to our processing of your personal information. Please note that your withdrawal will only take effect for future processing and will not affect the lawfulness of processing before the withdrawal.

If you would like to exercise any of these rights, please contact us as set forth in "Compliance@iATMGroup.com" below. We will process such requests in accordance with applicable laws. Please note that technical restrictions inherent in the blockchain may make certain requests difficult or impossible (e.g., deletion).

We may access, preserve, and disclose any information we store associated with you to external parties if we, in good faith, believe doing so is required or appropriate to: comply with law enforcement or national security requests and legal process, such as a court order or subpoena; protect your, our, or others' rights, property, or safety; enforce our policies or contracts; collect amounts owed to us; or assist with an investigation or prosecution of suspected or actual illegal activity.

SECURITY OF YOUR INFORMATION

We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy. Unfortunately, no system is 100% secure, and we cannot ensure or warrant the security of any information you provide to us. To the fullest extent permitted by applicable law, we do not accept liability for unauthorized access, use, disclosure, or loss of personal information.

By using our Services or providing personal information to us, you agree that we may communicate with you electronically regarding security, privacy, and administrative issues relating to your use of our Services. If we learn of a security system's breach, we may attempt to notify you electronically by posting a notice on our Services, by mail, or by sending an email to you.

INTERNATIONAL DATA TRANSFERS

All information processed by us may be transferred, processed, and stored anywhere in the world, including, but not limited to, the United States or other countries, which may have data protection laws that are different from the laws where you live. We endeavor to safeguard your information consistent with the requirements of applicable laws.

If we transfer personal information which originates in the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under applicable data protection laws, one of the safeguards we may use to support such transfer is the EU Standard Contractual Clauses.

For more information about the safeguards we use for international transfers of your personal information, please contact us as set forth below.