KIPLING SECURE INC.

PRIVACY POLICY

Last Updated: __March 26_____, 2024

WE WILL POST ANY CHANGES TO THIS PRIVACY POLICY IN A NOTICE OF THE CHANGE AT THE BOTTOM OF OUR WEB PAGE WITH A HYPERLINK THERETO. PLEASE REGULARLY REVIEW THIS PRIVACY POLICY. NOTWITHSTANDING IF YOU CONTINUE TO USE OUR SERVICES, YOU ARE BOUND BY ANY CHANGES THAT WE MAKE TO THIS PRIVACY POLICY.

1. INTRODUCTION

Kipling Secure Inc. ("Kipling Secure," "we," "us," or "our") respects the privacy of its Users ("User," "your," or "you"). This Privacy Policy (the "Privacy Policy") explains how we collect, use, disclose, and safeguard your information when you use Kipling Secure Platform (the "Platform") through Kipling Secure's website at https://kiplingsecure.ai/ (the "Website").

Kipling Secure is committed to protecting the privacy of its Users whose information is collected and stored while using Kipling Secure's Platform through our Website or App. This Privacy Policy is applicable to our Website, Platform and all applications offered for sale to the public.

The capitalized terms have the same meaning as ascribed in our Terms of Service as applicable, unless otherwise noted here.

PLEASE READ THIS PRIVACY POLICY CAREFULLY TO UNDERSTAND OUR POLICIES AND PRACTICES REGARDING YOUR INFORMATION AND HOW WE WILL TREAT IT. BY ACCESSING OR USING OUR WEBSITE AND PLATFORM, YOU AGREE TO ACCEPT ALL THE TERMS CONTAINED IN THIS PRIVACY POLICY AND ACKNOWLEDGE AND AGREE WITH THE PRACTICES DESCRIBED HEREIN. IF YOU DO NOT AGREE WITH THE TERMS OF THIS PRIVACY POLICY, PLEASE DO NOT ACCESS AND USE OUR WEBSITE AND PLATFORM.

IF YOU HAVE ANY QUESTIONS REGARDING THIS PRIVACY POLICY, PLEASE SEND US AN EMAIL AT PRIVACY@KIPLINGSECURE.AI.

WE DO NOT SELL YOUR PERSONAL INFORMATION, NOR DO WE INTEND TO DO SO. WE DO NOT GIVE ACCESS TO YOUR PERSONAL INFORMATION TO THIRD PARTIES EXCEPT TO SUBPROCESSORS TO ASSIST US IN THE PROVISION OF OUR SERVICES TO YOU.

2. WHAT INFORMATION DO WE COLLECT?

When you register to use our Website or Platform, we collect personal information (also referred to as personally identifiable information or "PII") which may include your name, address, online contact information such as your email address or username, phone number, and other personal information. The information so collected will be stored on our servers. You are able to change your personal information via email by contacting us at privacy@kiplingsecure.ai or through your profile or account settings on our Website or Platform.

a. Geolocation and Equipment Information. We may collect information that does not personally identify you such as (i) your geolocation, and (ii) information about your internet connection, the equipment you use to access our Website or Platform, and usage details.

b. Financial Information. We currently do not collect or store any credit cards or bank information, as we are using a third-party payment processor. However, we will update this Privacy Policy when we start using and storing such information. We will also inform you via reasonable means if we start collecting such information from you.

3. HOW DO WE COLLECT INFORMATION?

We collect personal information from you in the following ways:

a. At registration on our Website or Platform;
b. In email, text, and other electronic messages between you and our Website or Platform;
c. Through mobile and desktop applications your downloads from our Website or Platform, which provides dedicated non-browser based interaction between you and our Website or Platform;
d. When you interact with our advertising and applications on third-party website and services, if those applications or advertising include a link to this Privacy Policy;
e. From you placing an order, which includes details of transactions you carry out on our Website or Platform;
f. When you subscribe to a newsletter;
g. From your responses to a survey;
h. From forms filled out by you;
i. From records or copies of correspondences (including email addresses) if you contact us;
j. From search queries on our Website or Platform; and
k. When you post information to be published or displayed on our Website or Platform.

We collect information from you automatically when you navigate through our Website or Platform in the following ways:

a. Usage details;
b. IP addresses;
c. Information obtained through browser cookies;
d. Information obtained through flash cookies;
e. Web beacons on our Website;
f. Web beacons on emails sent by us; and
g. Other tracking technologies.

4. HOW DO WE USE YOUR INFORMATION?

We use the information that you provide to:

a. Personalize your experience in using our Platform;
b. Provide you with information, products, or services requested from us;
c. Present our Website and Platform and their contents to you;
d. Provide you with notices about account and/or subscription, including expiration and renewal notices;
e. Carry out obligations and enforce rights arising from contracts entered into between you and us, including billing and collection;
f. Notify you about changes to our Website and Platform and any products or services;

g. Allow you to participate in interactive features on our Website and Platform;
h. Improve the Website and Platform;
i. Improve our customer service;
j. Administer contests, promotions, and surveys or other Website and Platform features;
k. Process transactions;
l. Anonymize data and aggregate data for statistics;
m. Contact you for other purposes with your consent;
n. Contact you about our products and services that may be of interest;
o. Contact you about third parties' goods and services;
p. Enable the display of advertisements to our advertisers' target audiences, although personal information is not shared with advertisers without your consent; and
q. Send you periodic emails, in accordance with the CAN-SPAM Act of 2003 as detailed in Section 13, via the email address provided by you to (i) send information, respond to inquiries, and/or other requests or questions; (ii) process orders and send information and updates pertaining to such orders; (iii) send additional information related to your product and/or service; and (iv) market to our mailing list or continue to send email to you after the original transaction has occurred.

5. OUR COOKIE POLICY

Cookies are small pieces of text used to store information on web browsers. Cookies are used to store and receive identifiers and other information on computers, phones, and other devices. Other technologies, including data we store on your web browser or device, identifiers associated with your device, and other software, are used for similar purposes. In this Privacy Policy, we refer to all of these technologies as "Cookies."

We use Cookies on our Website to (a) help remember and process items in the shopping cart, (b) understand and save your preferences for future visits, (c) keep track of advertisements, (d) compile aggregate data about site traffic and site interactions in order to offer better site experiences and tools in the future, and (e) allow trusted third-party services that track this information on our behalf. You can set your browser to refuse all or some browser Cookies, but it may affect your user experience. We honor Do Not Track signals and, if one is in place, we will not track, plant cookies, or use advertising.

We allow third party behavioral tracking and links to third-party web pages. Occasionally, at our discretion, we may include or offer third-party products or services on our Website or Platform. These third-party sites have separate and independent privacy policies. We, therefore, have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our Website or Platform and welcome any feedback at about these sites. Please contact us at privacy@kiplingsecure.ai.

6. HOW DO WE PROTECT INFORMATION WE COLLECT?

Our Website is reasonably scanned to meet or exceed PCI Compliance. Our Website receives regular security scans and penetration tests. Our Website also receives regular malware scans. In addition, our Website and App use an SSL certificate as an added security measure. We require username and passwords for our employees who can access your personal information that we store and/or process on our Platform and servers. In addition, we actively prevent third parties from getting access to your personal information that we store and/or process on our Platform and servers. We accept payment by credit card through a third party credit card processor on our behalf. We will implement reasonable security measures every time you (a) place an order, or (b) enter, submit, or access your information, (c) register, or (d) access our Platform, on our Website.

7. DATA SECURITY MEASURES.

a. Security Measures. We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to us is stored on our secure servers behind firewalls. The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our Website or Platform, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. Unfortunately, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted to our Website or Platform. Any transmission of personal information is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures contained on our Website or Platform.

b. Fair Information Practice Principles. In the event of a personal data breach, we will notify you within fifteen (15) days via (i) email and/or (ii) our Platform notification system on our Website. We agree to the individual redress principle, which requires that individuals have a right to pursue legally enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that that individuals have recourse to courts or a government agency to investigate and/or prosecute non-compliance by data processors.

8. DISCLOSURE OF PERSONAL INFORMATION

There are times when we may share Personal Information that you have shared with us may be shared by Kipling Secure with others to enable us to provide you over Services, including contractors, service providers, and third parties ("Partners"). This section discusses only how Kipling Secure may share such information with Partners. We will ensure that our Partners protect your Personal Information. The following describe how and with whom we may share your Personal Information:

Disclosure of Personal Information.

a. We may disclose aggregated, de-personalized information about you that does not identify any individual to other parties without restriction, such as for marketing, advertising, or other uses.
b. We may disclose personal information to our subsidiaries and affiliates.
c. We may disclose personal information to contractors, services providers, and other third parties.
d. We require all contractors, service providers, and other third parties to whom we disclose your personal information to be under contractual obligations to keep personal information confidential and to use it only for the purposes for which we disclose them.
e. We may disclose personal information in the event of a merger, sale of business, etc.
f. We may disclose to third parties to market their products and services to you if you have either consented or not opted out of these disclosures.
g. We may disclose personal information to third parties to market their products and services if you have either consented or not opted out of these disclosures.
h. We require all other Partners, to whom we disclose your personal information, to enter into contracts with us to keep personal information confidential and use it only for the purposes for which we disclose it to such Partners.
i. We may disclose personal information for any other purpose for which you have provided it.
j. We may only disclose personal information as described in this Privacy Policy or your consent.

Other Disclosure of Personal Information.

a. We will disclose personal information (i) to comply with any court order, law, or legal process, including to respond to any government or regulatory request, (ii) to enforce or apply our Terms of Service and other agreements, including for billing and collection purposes, (iii) if we believe it is necessary or appropriate to protect the rights, property, or safety of Kipling Secure, our customers or others, and/or (iv) if it is necessary or appropriate to protect the rights, property, or safety of Kipling Secure, our customers, or others, and this includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

Third Party Disclosure.

a. We do not sell, trade, rent, or otherwise transfer personal information to others, unless we provide you with advance notice. This does not include our hosting partners and other parties who assist us in operating our Website or Platform, conducting our business, or servicing you, so long as those parties agree to keep this information confidential.
b. We do not provide non-personally identifiable visitor information for marketing purposes.

Choices Users Have About How Kipling Secure Uses and Discloses Information.

a. Tracking Technologies and Advertising. You can set their browser to refuse some or all the browser cookies, but if youdisable or refuse cookies, some parts of our Website may not be accessible or function properly.

b. Disclosure of Users' Information for Third-Party Advertising. Users can opt-out by (i) checking the relevant form when we collect the data; (ii) logging into the Website or Platform and adjusting their preferences in their account profile by checking or unchecking the relevant boxes, or (iii) emailing us their opt-out request at privacy@kiplingsecure.ai. Users receiving promotional email can opt-out by sending a return email requesting to be omitted from future promotional email distributions. This opt-out will not apply to information provided by Kipling Secure for product purchases, warranty registration, or other transactions.

c. Disclosure of User's Information for Targeted Advertising. Users can opt-out by (i) checking the relevant form when we collect the data, (ii) logging into the Website or Platform and adjusting their preferences in their account profile by checking or unchecking the relevant boxes, or (iii) emailing us their opt-out request at privacy@kiplingsecure.ai.

9. GOOGLE ADSENSE AND GOOGLE ANALYTICS

Google, as a third-party vendor, uses Cookies to serve advertisements to Users on our Website and Platform. Google uses first-party Cookies, such as Google Analytics Cookies, to compile data regarding User interactions with ad impressions and other ad service functions as they relate to our Platform. We currently use Google Analytics to collect and process certain Website usage data. To learn more about Google Analytics and how to opt-out, please visit https://policies.google.com/privacy/google-partners.

We have implemented advertising features on our Website and Platform including: (a) remarketing with Google AdSense; (b) Google Display Network Impression Reporting; (c) Google Demographics and Interests Reporting; and (d) Google's DoubleClick platform integration.

We use these Cookies to compile data regarding User interactions with ad impressions and other ad service functions as they relate to our Website.

10. FOR OUR EUROPEAN CUSTOMERS AND VISITORS

We are headquartered in the United States. Most of the operations are located in the United States. Your Personal Information, which you give to us during registration or use of our Website or Platform, may be accessed by or transferred to us in the United States. If you are visiting our Web site or registering for our Services from outside the United States, be aware that your Personal Information may be transferred to, stored, and processed in the United States. Our servers or our third-party hosting services partners are located in the United States. By using our site, you consent to any transfer of your Personal Information out of Europe, UK, or Switzerland for processing in the US or other countries.

- If you are a resident of or a visitor to Europe, you have certain rights with respect to the processing of your Personal Data, as defined in the General Data Protection Regulation ("GDPR").
- Please note that in some circumstances, we may ask you to provide us with additional information in connection with your request, which may be Personal Data, for example, if we need to verify your identity or the nature of your request.
- In such situations, however, we will still respond to let you know of our decision.
- As used herein, "Personal Data" means any information that identifies you as an individual, such as name, address, email address, IP address, phone number, business address, business title, business email address, company, etc.

a. EU Standard Contractual Clauses. On June 4, 2021, the EU promulgated a new set of SCCs (the "New SCCs"), which replaced the old SCCs which had been in place for over a decade. We now comply with the New SCCs with respect to the transfer of Personal Data from the EU to the US and other countries for Processing, as defined in the GDPR. If there is any conflict between the terms and conditions in this Privacy Policy and your rights under the New SCCs, the terms and conditions in the new SCCs will govern.

b. The New SCCs.

- The New SCCs took effect on June 27, 2021.
- The Old SCCs may still be used for new data transfers in new contracts during a three-month transition period that ends on September 27, 2021.
- Existing data transfers contracts that rely on the Old SCCs can be used until December 27, 2022, by which time all data transfers relying on the Old SCCs must be transitioned to the New SCCs.
- As of now, we and our customers are using the New SCCs to transport Personal Data from the EU to other countries including the US for processing by us.
- You are the Controller, as defined in the GDPR, and the Exporter, as defined in the New SCCs, of the Personal Data and we are a processor, as defined in the GDPR, and the Importer of such Personal Data.
- You agree to comply with the GDPR rules that apply to Controllers and the New SCCs rules that apply to Data Exporters. We agree to comply with the GDPR rules that apply to Processors and the New SCCs rules that apply to Data Importers.

c. Our GDPR Compliance Commitment.

- We agree to fully comply with the letter and the spirit of the GDPR and the New SCCs with respect to the transfer or your Personal Data for Processing outside the EU.
- As a Data Importer, a User may contact us as set forth in Subsection 9(d) below with respect to the Personal Data we store and process on you.
- We hereby notify you that we will be processing, as defined in the GDPR, the Personal Data of your Authorized Users (i.e., those individuals whom you have authorized to access our Platform

and to use our Services) in the US, Canada, and Turkey for us to be able to provide the Services to you that we have agreed to do in our definitive service agreement between you and us.

- Upon request, we will provide you with a list of your Personal Data that we will process and a copy of the New SCCs under which we will transport your Personal Data for processing.
- We hereby warrant that, at the time of agreeing to the SCCs for the transport of your Personal Data, we have no reason to believe that the laws and practices applicable to us as a data processor and a data importer, including those of the US, Canada, and Turkey are not in line with the requirements of the New SCCs.
- If we cannot satisfy any request or dispute to your satisfaction, we will agree to arbitrate or litigate the dispute in the EU jurisdiction in which your reside.
- We will only transfer your Personal Data to a third country in accordance with documented instructions from you.
- Your Personal Data will be transferred and stored in an encryption format.
- Only our employees, who have a need to access your Personal Data to enable us to meet our contractual and legal obligations to you, will be given access to your Personal Data.
- Such employees will be given a User Name and Password to access your Personal Data.
- We will keep an automated record of all persons who have accessed your Personal Data.

d. Rights of Data Subjects. To make any of the following requests, with respect to this Privacy Policy, our Terms or Use, and/or Personal Data, please contact us via email at privacy@kiplingsecure.ai.

i. Access: You can request more information about the Personal Information we hold about you. You can also request a copy of the Personal Information.

ii. Rectification: If you believe that any Personal Information we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data. Please contact us as soon as possible upon noticing any such inaccuracy or incompleteness.

iii. Objection: You can contact us to let us know that you object to the collection or use of your Personal Information for certain purposes.

iv. Erasure: You can request that we erase some or all of your Personal Information from our systems.

v. Restriction of Processing: You can ask us to restrict further processing of your Personal Information.

vi. Portability: You have the right to ask for a copy of your Personal Information in a machine-readable format. You can also request that we transmit the data to another entity where technically feasible.

vii. Withdrawal of Consent: If we are processing your Personal Information based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time. Please note, however, that if you exercise this right, it may limit your ability to use some/ all of our Services or Platform and you may have to then provide express consent on a case-by-case basis for the use or disclosure of certain of your Personal Information, if such use or disclosure is necessary to enable you to utilize some or all of our Services and Platform.

viii. Right to File Complaint: You have the right to lodge a complaint about our practices with respect to your Personal Information with the supervisory authority of your country or EU Member State. Please go to https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm to locate your Data Protection Authority in the EU. You may contact the UK's Information Commissioner at https://ico.org.uk/make-a-complaint or by telephone: 0303 123 1113.

ix. We will respond to your inquiry within thirty (30) days of the receipt.

11. YOUR CALIFORNIA PRIVACY RIGHTS

Kipling Secure does not sell, trade, or otherwise transfer to outside third parties your "Personal Information" as the term is defined under the California Civil Code Section § 1798.82(h). Additionally, California Civil Code Section § 1798.83 permits Users of our Website or Platform that are California residents to request certain information regarding our disclosure of their Personal Information to third parties for their direct marketing purposes. To make a request for such disclosure, or identification and/or deletion of Personal Information in all our systems that we store on you, please send an email to privacy@kiplingsecure.ai.

Note that (i) if we delete your Personal Information as requested, we will no longer be able to provide our services to you and (ii) we may need to keep such Personal Information for a while during the shutting down and billing process. If you would like to discuss our Personal Information storage and processing process with us, please send us an email at privacy@kiplingsecure.ai.

12. COPPA COMPLIANCE (FOR CHILDREN UNDER 13 USERS ONLY)

The Children's Online Privacy Protection Act ("COPPA") is a federal legislation that applies to entities that collect and store "Personal Information," as the term is defined under COPPA, from children under the age of 13. We are committed to ensure compliance with COPPA. Our Website and Platform are not meant for use by children under the age of 13. Our Website and Platform do not target children under the age of 13, but we do not age-screen or otherwise prevent the collection, use, and personal disclosure of persons identified as under 13. If you would like to know more about our practices and specifically our practices in relation to COPPA compliance, please email us at privacy@kiplingsecure.ai.

IF YOU ARE UNDER 13, PLEASE DO NOT ACCESS OR USE OUR WEBSITE OR PLATFORM.

13. CAN-SPAM ACT OF 2003

The CAN-SPAM Act establishes requirements for commercial messages, gives recipients the right to have businesses stop emailing them, and spells out penalties for violations. Per the CAN-SPAM Act, we will:

a. not use false or misleading subjects or email addresses;
b. identify the email message as an advertisement in some reasonable way;
c. include the physical address of Kipling Secure, which is 108 W. 13TH STREET SUITE 100;
d. monitor third-party email marketing services for compliance, if one is used;
e. honor opt-out/unsubscribe requests quickly; and
f. give an "opt-out" or "unsubscribe" option.

If you wish to opt out of email marketing, follow the instructions at the bottom of each email or contact us at privacy@kiplingsecure.ai and we will promptly remove you from all future marketing correspondences.

14. MODIFICATIONS TO OUR PRIVACY POLICY

We will post any changes to this Privacy Policy in a notice of the change at the bottom of our web page with a hyperlink thereto. We will also send you an email describing such changes. Please regularly review this Privacy Policy. Notwithstanding if you continue to use our services, you are bound by any changes that we make to this Privacy Policy.

15. LIST OF THIRD-PARTY SERVICE PROVIDERS

Kipling Secure uses the following third-party service providers for the provision of services as detailed under the Terms of Service, as applicable

Name of Third-Party Service Provider	Contact Information
Amazon Web Services Inc. (North Virginia, US)	Website: https://aws.amazon.com/premiumsupport/knowledge-center/aws-phone-support/ Address: 410 Terry Avenue North, Seattle, WA 98109-5210
Stripe, Inc.	Email: info@stripe.com Address: 510 Townsend St, San Francisco, CA 94103
Google Cloud	Website: www.support@google.com Telephone: (855) 817-0841
Microsoft Azure	Website: https://support.microsoft.com/en-us/contactus/ Address: 1 Microsoft Way, Redmond, WA 98052-6399
PayPal	Website: https://www.paypal.com/us/smarthelp/contact-us Address: 2211 North First Street San Jose, CA 95131

Additionally, if you have any questions or concerns about our third-party service providers, please email us at privacy@kiplingsecure.ai.

16. COPYRIGHT INFRINGEMENT/DMCA NOTICE

If you believe that any content on our Website or Platform violates your copyright, and you wish to have the allegedly infringing material removed, the following information in the form of a written notification (pursuant to the Digital Millennium Copyright Act of 1998 ("DMCA Takedown Notice")) must be provided to our designated Copyright Agent.

a. Your physical or electronic signature;
b. Identification of the copyrighted work(s) that you claim to have been infringed;
c. Identification of the material on our Website or Platform that you claim is infringing and that you request us to remove;
d. Sufficient information to permit us to locate such material;
e. Your address, telephone number, and email address;
f. A statement that you have a good faith belief that use of the objectionable material is not authorized by the copyright owner, its agent, or under the law; and
g. A statement that the information in the notification is accurate, and under penalty of perjury, that you are either the owner of the copyright that has allegedly been infringed or that you are authorized to act on behalf of the copyright owner.

Kipling Secure's Copyright Agent to receive DMCA Takedown Notices is Saurabh Sandhir, at privacy@kiplingsecure.ai and at Kipling Secure, Attn: DMCA Notice, 108 W. 13TH STREET SUITE 100. You acknowledge that for us to be authorized to take down any content, your DMCA Takedown Notice must comply with all the requirements of this Section. Please note that, pursuant to 17 U.S.C. § 512(f), any misrepresentation of material fact (falsities) in a written notification automatically subjects the complaining party to liability for any damages, costs and attorney's fees incurred by Kipling Secure in connection with the written notification and allegation of copyright infringement.

17. ANTI-BRIBERY COMPLIANCE

Kipling Secure represents and warrants that it is fully aware of and will comply with, and in the performance of its obligations hereunder will not take any action or omit to take any action that would cause it or its customers to be in violation of, (i) U.S. Foreign Corrupt Practices Act, (ii) U.K. Anti-Bribery Act, (iii) India Prevention of Corruption Act of 1988, or (iv) any other applicable anti-bribery statutes and regulations, and (v) any regulations promulgated under any such laws. Company represents and warrants that neither it nor any of its employees, officers, or directors is an official or employee of any government (or any department, agency or instrumentality of any government), political party, state owned enterprise or a public international organization such as the United Nations, or a representative or any such person (each, an "Official"). Company further represents and warrants that, to its knowledge, neither it nor any of the Supplier Personnel has offered, promised, made or authorized to be made, or provided any contribution, thing of value or gift, or any other type of payment to, or for the private use of, directly or indirectly, any Official for the purpose of influencing or inducing any act or decision of the Official to secure an improper advantage in connection with, or in any way relating to, (A) any government authorization or approval involving Kipling Secure,, or (B) the obtaining or retention of business by Kipling Secure. Supplier further represents and warrants that it will not in the future offer, promise, make or otherwise allow to be made or provide any payment and that it will take all lawful and necessary actions to ensure that no payment is promised, made or provided in the future by any of the Supplier Personnel.

18. CONTACT US

To ask questions or comment about this Privacy Policy and our privacy practices, contact us at:

- Privacy Officer
- Email: privacy@kiplingsecure.ai
- Address: Kipling Secure, 108 W. 13TH STREET SUITE 100

PLEASE NOTE: IF YOU USE OUR WEBSITE OR PLATFORM, YOU HAVE AGREED TO AND ACCEPTED THE PRACTICES DESCRIBED IN THIS PRIVACY POLICY AND THE TERMS AND CONDITIONS SET FORTH IN OUR TERMS OF SERVICE, AS APPLICABLE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS PRIVACY POLICY OR OUR TERMS OF SERVICE, PLEASE DO NOT USE OUR WEBSITE OR PLATFORM.