OMEN FUNDED TRADING GDPR POLICY

Last Updated: May 27, 2026

Welcome to Omen Funded Trading. This Privacy Policy (the "**Policy**") explains how Dory TradeCo Ltd., a Cayman Islands exempted company ("**we**", "**us**", "**our**" or the "**Controller**"), collects, uses, discloses, and otherwise processes the personal data of natural persons located in the European Economic Area (the "**EEA**"), the United Kingdom and Switzerland (collectively, the "**Relevant Jurisdictions**") in connection with our mobile applications, websites and any other online services that reference or link to this Policy (the "**Services**").

This Policy is issued pursuant to, and shall be construed in accordance with, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**EU GDPR**"), the United Kingdom General Data Protection Regulation as incorporated by the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, the "**UK GDPR**"), the Swiss Federal Act on Data Protection (the "**FADP**"), and any successor, replacement, supplementing or implementing legislation in force from time to time (together, "**GDPR**" or "**Applicable Data Protection Law**"). For the purposes of GDPR, we act as the data controller in respect of the personal data we process, unless otherwise indicated. In certain limited circumstances, we may process personal data jointly with our affiliates or business partners as joint controllers within the meaning of Article 26 GDPR, or as processors on behalf of another controller within the meaning of Article 28 GDPR; in such cases, the essence of any joint controller arrangement is available upon written request to the extent required by Applicable Data Protection Law.

You may contact us at support@nemotrading.xyz.

This Policy does not address our privacy practices relating to Omen Funded Trading job applicants, employees, contractors, agents, advisors, or other employment-related individuals (which are addressed in a separate notice), nor any data that is not subject to Applicable Data Protection Law (such as anonymised, deidentified, statistical or aggregate data that cannot reasonably be associated with an identified or identifiable natural person, or publicly available information to the extent excluded from the scope of Applicable Data Protection Law). This Policy is not a contract and does not create any legal rights or obligations beyond those expressly provided by Applicable Data Protection Law. To the maximum extent permitted by law, nothing in this Policy constitutes a waiver, modification or limitation of any defence, exemption, derogation, restriction or limitation available to us under Applicable Data Protection Law or any other applicable law.

EU, UK and Swiss Representatives

Where required by Article 27 of the EU GDPR, Article 27 of the UK GDPR and/or Article 14 of the FADP, we have appointed, or will appoint, representatives in the EEA, the United Kingdom and Switzerland (each, a "**Representative**"). The current contact details of our Representatives are available upon written

request to support@nemotrading.xyz. The appointment of a Representative is without prejudice to, and does not affect or limit, our own legal responsibility or liability under Applicable Data Protection Law, and does not in itself create any direct legal relationship between you and the Representative beyond that which is mandated by Applicable Data Protection Law.

Data Protection Officer

Where the appointment of a Data Protection Officer is mandatory under Article 37 of the EU GDPR or the UK GDPR, we have appointed, or will appoint, a Data Protection Officer (the "**DPO**"), who may be contacted at support@nemotrading.xyz. Where appointment is not mandatory, we have nonetheless designated an internal privacy contact for the supervision of compliance with Applicable Data Protection Law.

Lawful Bases for Processing Personal Data

Under Article 6(1) of GDPR, we may only process personal data where one or more of the following lawful bases apply. The specific lawful basis (or bases) we rely on depends on the processing activity, the purpose, and the categories of personal data concerned, and may vary from time to time. The principal lawful bases we rely on include:

- **Consent (Article 6(1)(a))**: where you have given freely-given, specific, informed and unambiguous consent to the processing of your personal data for one or more specific purposes;
- **Contract (Article 6(1)(b))**: where processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request prior to entering into a contract;
- **Legal Obligation (Article 6(1)(c))**: where processing is necessary for compliance with a legal obligation to which we are subject, including, without limitation, anti-money laundering, counter-terrorism financing, sanctions, "know your customer", tax, accounting, financial services regulatory, recordkeeping, audit, reporting, court and competent authority orders, and similar legal and regulatory obligations imposed by any competent authority in any jurisdiction to which we are subject or in which we operate;
- **Vital Interests (Article 6(1)(d))**: where processing is necessary to protect your vital interests or the vital interests of another natural person;
- **Public Interest (Article 6(1)(e))**: where processing is necessary for the performance of a task carried out in the public interest, including the prevention and detection of fraud, financial crime, sanctions violations, market abuse and other unlawful conduct; and
- **Legitimate Interests (Article 6(1)(f))**: where processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, provided such interests are not overridden by your interests or fundamental rights and freedoms requiring protection of personal data. We have conducted, and continue to conduct from time to time, appropriate legitimate interests

assessments ("**LIAs**") in respect of processing carried out on this basis and have determined that our legitimate interests prevail in respect of the relevant processing. Our legitimate interests include, without limitation: operating, securing, monitoring, maintaining, supporting and improving the Services; preventing fraud, abuse, money-laundering and other illegal or harmful conduct; enforcing our terms, policies and agreements; conducting research, analytics and product development; protecting the rights, property and safety of us, our affiliates, our users and third parties; ensuring business continuity and operational resilience; complying with foreign laws, regulations and regulator expectations; conducting due diligence; conducting and supporting corporate transactions; and operating, financing and growing our business. A summary of any applicable LIA is available upon written request to the extent required by Applicable Data Protection Law.

Where processing involves "special category" personal data within the meaning of Article 9(1) GDPR (for example, biometric data processed for the purpose of uniquely identifying you, or data revealing certain protected attributes), we rely on one or more additional conditions under Article 9(2), including: (a) your explicit consent; (b) processing necessary for the performance of obligations and the exercise of specific rights in the field of employment, social security and social protection law; (c) processing necessary to protect vital interests; (d) processing necessary for the establishment, exercise or defence of legal claims; (e) processing necessary for reasons of substantial public interest, on the basis of applicable EU, UK, Member State or Swiss law (including, without limitation, anti-money laundering, counter-terrorism financing and fraud prevention legislation); or (f) processing necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) GDPR. Where processing relates to personal data concerning criminal convictions and offences within the scope of Article 10 GDPR, we process such data only to the extent authorised by Applicable Data Protection Law.

Our Collection and Use of Personal Data

The categories of personal data we collect depend on how you interact with us and the Services. For example, you may provide us with personal data directly when you sign up for our mailing list, register for an account, conduct or simulate a transaction, submit content, post a review or testimonial, participate in an event, contest, promotion or survey, or otherwise contact us or interact with us.

We also collect personal data automatically when you interact with our websites and other Services and may also collect personal data from other sources and third parties as described below.

The Services may evolve over time, and the nature of the personal data we collect and process may change accordingly, subject to this Policy and Applicable Data Protection Law. Any material change to the processing activities described in this Policy will be communicated in accordance with Applicable Data Protection Law.

Personal Data Provided by Individuals

We collect the following categories of personal data that individuals provide to us:

- **Account Information**, including first and last name, email address, phone number, and account credentials or one-time passcodes. In some instances, we may collect your wallet address when you have been approved for Signal Provider status. We use this information primarily to administer your account, provide you with access to demo accounts, communicate with you regarding your account and your use of the Services, and for support purposes. **Lawful bases**: contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f)).
- **Contact Information**, including phone number, email address, mailing address, and communication preferences. We use this information primarily to fulfil your request or transaction, to communicate with you directly, and to send you marketing communications in accordance with your preferences and applicable law. **Lawful bases**: contract (Article 6(1)(b)), consent (Article 6(1)(a)) where required for direct electronic marketing under the ePrivacy Directive, PECR or other applicable law, and legitimate interests (Article 6(1)(f)).
- **Know Your Customer Information**, such as date of birth, proof of address, government-issued identification numbers, identification documents, photographs, and the results of automated checks, including sanctions screening, politically-exposed-person screening, adverse media screening and liveness checks, and (where applicable) biometric data processed solely for the purpose of identity verification by us or our identity-verification providers. We use this information to verify your identity, assess your eligibility to use the Services, and discharge our legal and regulatory obligations. **Lawful bases**: legal obligation (Article 6(1)(c)), substantial public interest under Article 9(2)(g) (with respect to biometric and special category data), legitimate interests (Article 6(1)(f)), and (with respect to biometric data, where applicable) explicit consent (Article 9(2)(a)).
- **Simulated Transaction Information**, including simulated transaction amount, type and nature of the simulated transaction, time and date of the simulated transaction, position data, performance metrics, and risk metrics. We use this information to process and administer simulated transactions, assess your performance on evaluations or challenges, maintain simulated transaction records, provide and improve the Services, detect and prevent fraud, comply with legal and regulatory obligations, train, fine-tune, evaluate and improve our and our third-party providers' artificial intelligence and machine learning models, and otherwise manage our relationship with you. **Lawful bases**: contract (Article 6(1)(b)), legitimate interests (Article 6(1)(f)), and legal obligation (Article 6(1)(c)).
- **Professional Information**, including job title, company name, professional background, source of funds and source of wealth declarations, and the nature of your relationship with us. We use this information primarily to fulfil your request or transaction, to determine how we communicate

with you, to administer your account, to provide you with the Services, and for contractor support purposes. **Lawful bases**: contract (Article 6(1)(b)), legal obligation (Article 6(1)(c)) and legitimate interests (Article 6(1)(f)).

- **Uploaded Content**, including any files, documents, audio, videos, images, data, or communications you choose to input, upload, or transmit to the Services. We use this content primarily to provide the Services, to facilitate your requests, and to improve the Services (including by training, fine-tuning, evaluating and improving our and our third-party providers' artificial intelligence and machine learning models). To the extent any Uploaded Content contains personal data relating to any third party, you represent and warrant to us that you have a lawful basis under Applicable Data Protection Law to disclose such personal data to us and to permit our processing thereof in accordance with this Policy, and you agree to indemnify and hold us harmless against any claims, losses, damages, costs and expenses arising out of or in connection with any breach of such representation and warranty, to the maximum extent permitted by law. **Lawful bases**: contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f)).
- **Payment Information**, including wallet address. We use this information for KYC purposes and to provide Signal Providers with compensation or profit allocation. **Lawful bases**: legal obligation (Article 6(1)(c)), contract (Article 6(1)(b)) and legitimate interests (Article 6(1)(f)).
- **Event, Promotion, and Survey Information**, including information provided when you sign up for an event, enter a promotion, complete a survey or submit a testimonial. We use this information primarily to administer and facilitate the Services, respond to your submission, communicate with you, conduct market research, inform our marketing and advertising activities, improve and grow our business, and facilitate the related event, promotion or survey. **Lawful bases**: contract (Article 6(1)(b)), consent (Article 6(1)(a)) and legitimate interests (Article 6(1)(f)).
- **Security-Related Information**, including name and contact information of visitors to our premises, video recordings of premises, and electronic login records and access details when a visitor uses company technology on our premises. We use this information primarily to protect the security of our premises, employees, and our company. **Lawful bases**: legitimate interests (Article 6(1)(f)) and legal obligation (Article 6(1)(c)).
- **Feedback and Support Information**, including the contents of custom messages sent through forms, chat platforms (including online live chat or automated chat functions), email addresses, or other contact information we make available to users, as well as recordings of calls with us, where permitted by law (including through the use of automated or artificial intelligence tools provided by us or our third-party providers). We use this information primarily to investigate and respond to your inquiries, to communicate with you via online chat, email, phone, text message or social media, to improve the Services, and to train, fine-tune, evaluate and improve our and our third-party providers' artificial intelligence and machine learning models. **Lawful bases**:

contract (Article 6(1)(b)), legitimate interests (Article 6(1)(f)), legal obligation (Article 6(1)(c)) and (where required) consent (Article 6(1)(a)).

We take reasonable steps to limit the personal data we collect to what is necessary for the purposes described in this Policy in accordance with the principle of data minimisation under Article 5(1)(c) GDPR. However, due to the nature of the Services and the legal and regulatory obligations to which we are subject, certain data collection may be inherent to system functionality, eligibility assessment, and regulatory compliance.

Statutory or Contractual Requirement (Article 13(2)(e) GDPR). Certain categories of personal data are required by law or contract or are a requirement necessary to enter into a contract. If you do not provide personal data that is required for us to provide the Services or to comply with our legal, regulatory, tax, sanctions, anti-money laundering, counter-terrorism financing or other compliance obligations, we may be unable to onboard or engage with you, transact with you, provide the relevant Services, process rewards or distributions, or otherwise respond to your request, and we may be required to suspend, restrict, or terminate any existing relationship, in whole or in part, in accordance with Applicable Data Protection Law and our other contractual and regulatory obligations.

Personal Data Automatically Collected

We, and our third-party partners, automatically collect information you provide to us and information about how you access and use the Services when you engage with us. We typically collect this information through the use of a variety of our own and our third-party partners' automatic data collection technologies, including (i) cookies or small data files that are stored on an individual's computer or device and (ii) other, related technologies, such as web beacons, pixels, embedded scripts, mobile SDKs, location-identifying technologies and logging technologies. Information we collect automatically about you may be combined with other personal data we collect directly from you or receive from other sources.

We may use IP address, device, network, location and related technical information to assess eligibility, enforce geographic and jurisdictional restrictions, detect attempts to circumvent access controls, comply with sanctions and other legal or regulatory requirements, and protect us from being regarded as carrying on regulated activity in any jurisdiction. Such processing is necessary for compliance with our legal obligations (Article 6(1)(c)), for the performance of a contract (Article 6(1)(b)) and for our legitimate interests in preventing unlawful and prohibited activity (Article 6(1)(f)).

We, and our third-party partners, use automatic data collection technologies to automatically collect the following data when you use the Services or otherwise engage with us:

- **Information About Your Device and Network**, including the device type, manufacturer, and model, operating system, IP address, browser type, Internet service provider, and unique identifiers associated with you, your device, or your network (including, for example, a persistent device identifier or advertising ID). We employ third-party technologies designed to allow us to

recognise when two or more devices are likely being used by the same individual and may leverage these technologies (where permitted by law) to link information collected from different devices.

- **Information About the Way Individuals Use the Services and Interact With Us**, including the site from which you came, the site to which you are going when you leave the Services, how frequently you access the Services, whether you open emails or click the links contained in emails, whether you access the Services from multiple devices, and other browsing behaviour and actions you take on the Services (such as the pages you visit, the content you view, videos you watch, the communications you have through the Services, and the content, links and ads you interact with). We employ third-party technologies designed to allow us to collect detailed information about browsing behaviour and actions that you take on the Services, which may record your mouse movements, scrolling, clicks, and keystroke activity on the Services and other browsing, search or purchasing behaviour. These third-party technologies may also record information you enter when you interact with our products or Services, or engage in chat features or other communication platforms we provide.
- **Information About Your Location**, including general geographic location that we or our third-party providers may derive from your IP address or other location-identifying technologies.

All of the information collected automatically through these tools allows us to improve your experience. For example, we may use this information to enhance and personalise your user experience, to monitor and improve the Services, to offer communications features, and to improve the effectiveness of our products, services, offers, advertising, communications and user service. We may also use this information to: (a) remember information so that you will not have to re-enter it during your visit or the next time you visit the site; (b) provide custom, personalised content and information, including targeted content and advertising (subject to your consent where required); (c) identify you across multiple devices; (d) provide and monitor the effectiveness of the Services; (e) monitor aggregate metrics such as total number of visitors, traffic, usage, and demographic patterns on our website; (f) diagnose or fix technology problems; and (g) otherwise plan for and enhance the Services. The lawful bases for this processing are legitimate interests (Article 6(1)(f)), contract (Article 6(1)(b)), and, for non-essential cookies and similar technologies, where required under the ePrivacy Directive (Directive 2002/58/EC), the Privacy and Electronic Communications Regulations 2003 ("**PECR**") or other applicable law, consent (Article 6(1)(a)).

For information about the choices you may have in relation to our use of automatic data collection technologies, please refer to the Your Privacy Choices section below and our separate Cookie Policy, where available.

Personal Data from Other Sources and Third Parties

We may receive the same categories of personal data as described above from the following sources and other parties:

- **Affiliates**: we may receive personal data from other entities and any affiliated entities where this is necessary for shared administration, compliance, service delivery, account management, internal reporting, risk management, and other purposes consistent with this Policy.
- **Service Providers**: we may receive personal data from service providers that perform services on our behalf, such as KYC, analytics, communications, identity verification, compliance, payment, survey, hosting and marketing providers, where this is necessary for the provision, operation, security, support or improvement of our products and Services. For example, we receive personal data you may submit in response to requests for KYC verification requirements or feedback to our survey providers.
- **Third-Party Technology and Compliance Providers**: we may receive personal data from non-affiliated technology, infrastructure, analytics, identity verification, wallet-screening, compliance, hosting, support and other service providers that support the operation, security, availability and compliance of the Services, including (without limitation) name, contact data, inferences about your preferences and attributes, and inferred fraud risk from identity verification and fraud prevention partners.
- **Financial Account Linking**: we may receive financial account information about you from third parties, such as wallet providers.
- **Single Sign-On**: we may provide you the ability to log in to the Services through certain third-party accounts you maintain. When you use these single sign-on protocols to access the Services, we do not receive your login credentials for the relevant third-party service. Instead, we receive tokens from the single sign-on protocol to help identify you in our system (such as by your username) and confirm that you have successfully authenticated through the single sign-on protocol.
- **Mobile Sign-On**: we may provide you the ability to log in to our mobile applications or authenticate yourself using facial, fingerprint, or other biometric recognition technology available through your mobile device. If you choose to utilise these login features, information about your facial geometry, your fingerprint, or other biometric information will be collected by your mobile device for authentication purposes. We do not store or have access to this biometric information. Instead, your mobile device will perform the biometric authentication process and only let us know whether the authentication was successful.
- **Employers**: if you interact with the Services in connection with your employment, we may obtain personal data about you from your employer or another company for which you work.
- **Other Users**: we may receive your personal data from our other users (for example, a user may provide us with your contact information as part of a referral).

- **Social Media**: when you interact with the Services through social media networks, we may receive information you permit the social network to share with third parties, dependent upon your privacy settings.
- **Advertisers, Influencers and Publishers**: advertisers, influencers, and publishers may share personal data with us in connection with our advertising efforts.
- **Other Sources**: we may also collect personal data about you from other sources, including publicly available sources, third-party data providers, sanctions and watch lists, regulatory and judicial bodies, and through corporate transactions such as mergers and acquisitions.
- **Inferences**: we may generate inferences or predictions about you and your interests and preferences based on the other personal data we collect and the interactions we have with you.

Where we obtain personal data from a source other than you, we will, to the extent required by Article 14 GDPR, provide you with the information specified therein within the time limits set out in Article 14(3), unless and to the extent that an exemption applies (including, without limitation, where you already have the information, where the provision of such information proves impossible or would involve a disproportionate effort, where obtaining or disclosure of the data is expressly laid down by Union, UK or Member State law, or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law).

You acknowledge that any use of the Services, including any features involving data processing, analytics, or AI-generated outputs, is undertaken at your own risk, and that we are not responsible for how you interpret, use, or rely on any such outputs.

Nothing in this Policy shall be construed as creating any fiduciary, advisory or special confidentiality relationship between you and us beyond those required by Applicable Data Protection Law.

Additional Uses of Personal Data; Compatible Further Processing

In addition to the primary purposes for using personal data described above, we may also use personal data we collect to, in each case on the lawful bases indicated:

- Fulfil or meet the reason the information was provided, such as to fulfil our contractual obligations, to facilitate payment for the Services, or to deliver the Services requested (**contract; legitimate interests**).
- Make automated decisions about you, including using artificial intelligence without initial human input, to evaluate your personal circumstances and other factors to predict risks or outcomes, such as fraud detection and KYC checks (**legal obligation; contract; legitimate interests; explicit consent where required under Article 22(2)(c)**).
- Manage our organisation and its day-to-day operations (**legitimate interests**).

- Verify your identity and eligibility for our products and Services, including as may be required for KYC, AML, sanctions, counter-terrorism financing, and other legal and regulatory due diligence requirements (**legal obligation; contract; legitimate interests; substantial public interest**).
- Communicate with you, including via email, text message, chat, social media and/or telephone calls (**contract; legitimate interests; consent for electronic direct marketing where required**).
- Facilitate the relationship we have with you and, where applicable, the company you represent (**contract; legitimate interests**).
- Request you provide us feedback about our product and Service offerings (**legitimate interests**).
- Address inquiries or complaints made by or about an individual in connection with our products or Services (**contract; legitimate interests; legal obligation**).
- Create and maintain accounts for our users (**contract**).
- Register you for and provide you access to events, sweepstakes, and surveys (**contract; consent; legitimate interests**).
- Market the Services to you, including through email, text message, push notification, and social media (**consent where required; legitimate interests**).
- Administer, improve, and personalise the Services, including by recognising you and remembering your information when you return to the Services (**legitimate interests; contract**).
- Develop, operate, improve, maintain, protect, and provide the features and functionality of the Services (including by training, fine-tuning, evaluating and improving our and our third-party providers' artificial intelligence and machine learning models) (**legitimate interests; contract**).
- Identify and analyse how you use the Services (**legitimate interests**).
- Infer additional information about you from your use of the Services, such as your interests (**legitimate interests**).
- Create aggregated, deidentified or anonymised information that cannot reasonably be used to identify you, which information we may use for purposes outside the scope of this Policy (**legitimate interests; such anonymised information, within the meaning of Recital 26 GDPR, falls outside the scope of GDPR**).
- Conduct research and analytics on our user base and the Services, including in furtherance of scientific or historical research and statistical purposes within the meaning of Article 89 GDPR (**legitimate interests; scientific research**).
- Test, enhance, update, and monitor the Services, or diagnose or fix technology problems (**legitimate interests**).

- Help maintain and enhance the safety, security, and integrity of our property, products, Services, technology, assets, and business (**legitimate interests; legal obligation**).
- Defend, protect, or enforce our rights or applicable contracts and agreements (including our Terms of Service), as well as to resolve disputes, to carry out our obligations and enforce our rights, and to protect our business interests and the interests and rights of third parties (**legitimate interests; establishment, exercise or defence of legal claims under Article 9(2)(f) where applicable**).
- Detect, prevent, investigate, or provide notice of security incidents or other malicious, deceptive, fraudulent, or illegal activity and protect the rights and property of Omen Funded Trading and others (**legitimate interests; legal obligation; substantial public interest**).
- Facilitate business transactions and reorganisations impacting the structure of our business (**legitimate interests**).
- Comply with contractual and legal obligations and requirements (**legal obligation; contract**).
- Fulfil any other purpose for which you provide your personal data, or for which you have otherwise consented (**consent**).

To the extent we further process personal data for a purpose other than that for which the personal data was originally collected, we will ascertain whether such further processing is compatible with the original purpose in accordance with Article 6(4) GDPR, taking into account, inter alia: (i) any link between the purposes for which the personal data was collected and the purposes of the intended further processing; (ii) the context in which the personal data was collected, in particular regarding the relationship between you and us; (iii) the nature of the personal data, in particular whether special categories of personal data are processed or whether personal data related to criminal convictions and offences are processed; (iv) the possible consequences of the intended further processing for you; and (v) the existence of appropriate safeguards. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 5(1)(b) GDPR, not be considered to be incompatible with the initial purposes.

As noted above, we may use your personal data to improve the Services and train, fine-tune, evaluate and improve the artificial intelligence and machine learning models that power our platform and Services.

Automated Decision-Making and Profiling

We use automated decision-making processes, including profiling, for purposes such as fraud detection, sanctions screening, politically-exposed-person screening, KYC and AML compliance, eligibility assessment, performance assessment, risk scoring, and similar legitimate and lawful purposes. Such automated decision-making may, in certain cases, produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22(1) GDPR.

Where automated decision-making is performed within the scope of Article 22 GDPR, we rely on one or more of the following grounds:

- the decision is necessary for entering into, or performance of, a contract between you and us (Article 22(2)(a));
- the decision is authorised by Union, UK or Member State law to which we are subject (including, without limitation, for the purpose of preventing fraud, money-laundering, terrorist financing or other financial crime) (Article 22(2)(b)); and/or
- the decision is based on your explicit consent (Article 22(2)(c)).

Subject to, and except where otherwise prohibited or restricted by, Applicable Data Protection Law, you have the right to: (a) obtain human intervention on our part; (b) express your point of view; and (c) contest the decision. Requests to exercise these rights should be submitted as set out in the Your Rights section below. We may decline a request where the decision falls outside Article 22, where an exemption or derogation applies, or where granting the request would prejudice our ability to comply with legal, regulatory or contractual obligations, or to prevent fraud, money-laundering or financial crime.

Our Disclosure of Personal Data

We disclose or otherwise make available personal data, on the lawful bases described above, as follows:

- **Third-Party Technology and Compliance Providers**: we may disclose personal data to non-affiliated technology, infrastructure, analytics, identity verification, wallet-screening, compliance, hosting, support and other service providers where reasonably necessary to operate, secure, support, monitor and improve the Services, administer accounts, conduct eligibility and compliance checks, and comply with applicable law.
- **Authorised Service Providers**: we disclose information about you with vendors who perform services for us, such as identification verification, fraud prevention, advertising, mailing services, tax and accounting services, contest fulfilment, web hosting, marketing, advertising, and analytics services. We require such processors to enter into written agreements that include the obligations required by Article 28(3) GDPR.
- **To Your Employer**: if you interact with the Services in connection with your employment, we may disclose personal data to your employer or another company for which you work.
- **To Marketing Providers**: we coordinate and share personal data with our marketing providers in order to advertise and communicate with you about the Services.
- **To Ad Networks and Advertising Partners**: we work with third-party ad networks and advertising partners to deliver advertising and personalised content on the Services, on other websites and services, and across other devices. Where required, such sharing is conducted on the basis of your consent, including through any applicable cookie consent banner.

- **To Business Partners**: we may share personal data with our business partners, or we may allow our business partners to collect personal data directly from you in connection with the Services. Where such partner is an independent controller, the partner's processing is governed by its own privacy notice.
- **In Connection with a Business Transaction or Reorganisation**: we may take part in or be involved with a business transaction or reorganisation, such as a merger, acquisition, joint venture, financing or sale of company assets. We may disclose, transfer, or assign personal data to a third party during negotiation of, in connection with, or as an asset in such a business transaction or reorganisation. In the unlikely event of our bankruptcy, receivership, or insolvency, your personal data may be disclosed, transferred, or assigned to third parties in connection with the proceedings or disposition of our assets.
- **To Facilitate Legal Obligations and Rights**: we may disclose personal data to third parties, such as legal advisors, courts, regulators and law enforcement: (i) in connection with the establishment, exercise, or defence of legal claims; (ii) to comply with laws or to respond to lawful requests and legal process; (iii) to protect our rights and property and the rights and property of our agents, contractors, and others, including to enforce our agreements, policies, and terms of use; (iv) to detect, suppress, or prevent fraud; (v) to reduce credit risk and collect debts owed to us; (vi) to protect the health and safety of us, our contractors, or any person; or (vii) as otherwise required, authorised or permitted by Applicable Data Protection Law. Such disclosures may include disclosure to authorities outside the Relevant Jurisdictions to the extent permitted by Applicable Data Protection Law.
- **With Your Consent or Direction**: we may disclose your personal data to certain other third parties or publicly with your consent or direction. For example, with your permission, we may post your testimonial on our websites.

We require all third parties that process personal data on our behalf to do so subject to confidentiality obligations and only for the specified purposes and in accordance with our written instructions, and to provide a level of protection at least equivalent to that required by Article 28 GDPR.

Retention of Personal Data

We retain personal data for as long as reasonably necessary for the purposes described in this Policy, in accordance with the storage limitation principle under Article 5(1)(e) GDPR. The criteria we apply to determine retention periods include:

- the duration of our ongoing relationship with you and the provision of the Services to you;
- our legal, regulatory, tax, accounting, sanctions, anti-money laundering, counter-terrorism financing, financial services, recordkeeping, audit and similar compliance obligations (which may

require retention for periods ranging from five (5) to ten (10) years or longer following termination of the relationship, depending on the jurisdiction and category of data);

- the existence, contemplation, or potential of legal claims, regulatory inquiries, investigations or disputes, and any applicable limitation periods;
- the necessity of the data for fraud prevention, security, and abuse prevention;
- the sensitivity of the personal data and the risks associated with processing; and
- any other legitimate business purpose consistent with this Policy and Applicable Data Protection Law.

We may retain certain information for longer than the foregoing periods where required or permitted by applicable law, including, without limitation, where deletion would impair legal, regulatory, security, fraud-prevention or compliance obligations, the establishment, exercise or defence of legal claims, or the legitimate operation of our business. Following expiry of the applicable retention period, we will either delete, anonymise or aggregate the personal data or, where deletion is not technically feasible or practicable, securely isolate the data from further active processing pending its eventual deletion.

Your Rights

Subject to, and in accordance with, Applicable Data Protection Law, including any exemptions, derogations, conditions and limitations set out therein, you have the following rights with respect to your personal data:

- **Right of access (Article 15 GDPR)**: to obtain confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, access to the personal data and certain related information.
- **Right to rectification (Article 16 GDPR)**: to have inaccurate personal data concerning you rectified, and to have incomplete personal data completed.
- **Right to erasure (Article 17 GDPR)** (the so-called "right to be forgotten"): to have personal data concerning you erased where the grounds in Article 17(1) apply, subject to the exemptions in Article 17(3) (including, without limitation, where processing is necessary for compliance with a legal obligation, for the establishment, exercise or defence of legal claims, for reasons of public interest in the area of public health, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes).
- **Right to restriction of processing (Article 18 GDPR)**: to obtain restriction of processing where the grounds in Article 18(1) apply.
- **Right to data portability (Article 20 GDPR)**: to receive personal data concerning you that you have provided to us, in a structured, commonly used and machine-readable format, and to transmit

such data to another controller, where processing is based on consent or contract and is carried out by automated means.

- **Right to object (Article 21 GDPR)**: to object, on grounds relating to your particular situation, to processing of personal data concerning you based on Article 6(1)(e) or (f); we will cease such processing unless we demonstrate compelling legitimate grounds which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.
- **Right to object to direct marketing (Article 21(2) GDPR)**: an absolute right to object at any time to processing of personal data concerning you for direct marketing purposes.
- **Rights related to automated decision-making (Article 22 GDPR)**: as further described under Automated Decision-Making and Profiling above.
- **Right to withdraw consent (Article 7(3) GDPR)**: where processing is based on consent, you may withdraw your consent at any time. Such withdrawal does not affect the lawfulness of processing based on consent before its withdrawal, nor does it affect processing based on a separate lawful basis.
- **Right to lodge a complaint (Article 77 GDPR)**: with a supervisory authority, in particular in the Member State of your habitual residence, place of work, or place of the alleged infringement. A list of EEA supervisory authorities is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en. UK residents may lodge a complaint with the Information Commissioner's Office (https://ico.org.uk/). Swiss residents may lodge a complaint with the Federal Data Protection and Information Commissioner (https://www.edoeb.admin.ch/).

To exercise any of your rights, please contact us as set forth in the Contact Us section below. We may request additional information from you to verify your identity before responding to your request, and we may decline to act on your request if we are unable to verify your identity to a reasonable standard. We are not obliged to comply with any request to the extent that compliance would: (i) require disclosure of personal data of other individuals; (ii) infringe the rights and freedoms of others (including trade secrets, intellectual property rights or confidentiality obligations); (iii) prejudice our ability to comply with legal, regulatory or contractual obligations; (iv) prejudice the prevention, detection or investigation of fraud, money laundering, terrorist financing or other financial crime; or (v) otherwise be excluded, restricted or limited under Applicable Data Protection Law. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request, in accordance with Article 12(5) GDPR.

We will respond to your request within the time limits set out in Article 12(3) GDPR (generally, one (1) month, extensible by up to two further months where necessary, taking into account the complexity and number of requests).

The exercise of any right under this section is without prejudice to our right to retain, use or disclose personal data as required or permitted by Applicable Data Protection Law.

Your Privacy Choices

Communication Preferences

- **Email Communication Preferences**: you can stop receiving promotional email communications from us by clicking on the "unsubscribe" link provided in any of our email communications. Please note that you cannot opt-out of service-related email communications (such as account verification, transaction confirmation, or service update emails).
- **Mobile Communication Preferences**: you can stop receiving promotional phone communications from us by informing the caller you no longer wish to receive promotional phone calls from us, following the instructions provided on the call for opting out of promotional phone calls (where available), or replying STOP to any one of our promotional text messages. Please note we may need to continue to communicate with you via phone for certain service-related messages (such as sending a verification code).
- **Push Notification Preferences**: you can stop receiving push notifications from us by changing your preferences in your device's notification settings menu or in the applicable service-specific application. We do not have any control over your device's notification settings and are not responsible if they do not function as intended.

Withdrawing Your Consent

Where we process your personal data on the basis of your consent under Article 6(1)(a) or Article 9(2)(a) GDPR, you may withdraw your consent at any time, in accordance with Article 7(3) GDPR, by following the instructions provided when your consent was requested or by contacting us as set forth in the Contact Us section below. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Withdrawal of consent for one purpose does not constitute withdrawal of consent for any other purpose or processing activity for which a separate lawful basis applies, and we may continue to process your personal data on any such other lawful basis.

Cookies and Automatic Data Collection Preferences

Where consent is required under the ePrivacy Directive, PECR or other applicable law for the use of cookies or similar technologies that are not strictly necessary for the provision of the Services, we will obtain such consent through an appropriate consent mechanism (such as a cookie consent banner). You may, at any time, withdraw or modify your cookie consent through the cookie preferences tool provided through the Services, where available.

You may also be able to utilise third-party tools and features to restrict our use of automatic data collection technologies. For example, (i) most browsers allow you to change browser settings to limit automatic data collection technologies on websites, (ii) most email providers allow you to prevent the

automatic downloading of images in emails that may contain automatic data collection technologies, and (iii) many devices allow you to change your device settings to limit automatic data collection technologies for device applications. Please note that blocking automatic data collection technologies through third-party tools and features may negatively impact your experience using the Services. We do not have any control over these third-party tools and features and are not responsible if they do not function as intended.

Targeted Advertising Preferences

We may engage third parties to help us facilitate targeted advertising designed to show you personalised ads based on predictions of your preferences and interests developed using personal data we maintain and personal data our third-party partners obtain from your activity over time and across nonaffiliated websites and other services. We may share a common account identifier (such as a hashed email address or user ID) with our third-party advertising partners to help link the personal data we and our third-party partners collect to the same person, or otherwise target advertising to an individual on a third-party website or platform.

In addition to taking the steps set forth in the Cookies and Automatic Data Collection Preferences section above, you may be able to further exercise control over the advertisements that you see by leveraging one or more targeted advertising opt-out programmes. For example:

- **Device-Specific Opt-Out Programmes**: certain devices provide individuals the option to turn off targeted advertising for the entire device (such as Apple devices through their App Tracking Transparency framework or Android devices through their opt-out of ads personalisation feature). Please refer to your device manufacturer's user guides for additional information.
- **European Interactive Digital Advertising Alliance**: individuals located in the EEA may opt out of receiving online interest-based targeted advertisements from participating companies via https://www.youronlinechoices.eu/.
- **Digital Advertising Alliance**: the Digital Advertising Alliance allows individuals to opt out via https://optout.aboutads.info/?c=2&lang=EN for browser-based advertising and https://www.youradchoices.com/appchoices for app-based advertising.
- **Network Advertising Initiative**: https://thenai.org/how-to-opt-out/.
- **Platform-Specific Opt-Out Programmes**: certain third-party platforms provide individuals the option to turn off targeted advertising for the entire platform.

Please note that when you opt out of receiving interest-based advertisements through one of these programmes, this does not mean you will no longer see advertisements from us or on the Services. Instead, it means that the online ads you do see from relevant programme participants should not be based on your interests. We are not responsible for the effectiveness of, or compliance with, any third parties' opt-out options or programmes or the accuracy of their statements regarding their programmes.

Partner-Specific Preferences

- **Device-Specific / Platform-Specific Preferences**: the device and/or platform you use to interact with us (such as your mobile device or social media provider) may provide you additional choices with regard to the data you choose to share with us. Please refer to your device or platform provider's user guides for additional information.
- **Google Analytics**: Google Analytics allows us to better understand how our website visitors interact with the Services. For information on how Google Analytics collects and processes data, as well as how you can control information sent to Google, review Google's website here: www.google.com/policies/privacy/partners/. You can learn about Google Analytics' currently available opt-outs, including the Google Analytics Browser Add-On, here: https://tools.google.com/dlpage/gaoptout/. You may control your advertising preferences or opt-out of certain Google advertising products by visiting the Google Ads Preferences Manager: https://myadcenter.google.com/?ref=help-center.

Children's Personal Data

The Services are not directed to, and we do not intend to, or knowingly, collect or solicit personal data from children. In accordance with Article 8 GDPR, in the EEA, where the processing of personal data of a child is based on consent in relation to the offer of information society services, such processing is lawful only where the child is at least sixteen (16) years old (or such lower age, not below thirteen (13), as set by the relevant Member State). In the United Kingdom, the corresponding minimum age is thirteen (13). Notwithstanding the foregoing, individuals under the age of eighteen (18), or below the age of majority in the jurisdiction in which they are using the platform or platform services, as applicable, are not permitted to subscribe to any of the Services.

If an individual is below the applicable age threshold, they should not use the Services or otherwise provide us with any personal data either directly or by other means. If a child has provided personal data to us, we encourage the child's parent or guardian to contact us to request that we remove the personal data from our systems. If we learn that any personal data we collect has been provided by a child under the applicable age threshold without the requisite parental or guardian consent or authorisation, we will promptly delete that personal data.

Security of Personal Data

We have implemented technical and organisational measures in accordance with Article 32 GDPR that are designed to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons. Such measures include, where appropriate: the pseudonymisation and encryption of personal data; measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; measures to

restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and processes for regularly testing, assessing and evaluating the effectiveness of such measures.

In addition, we take steps designed to ensure any third party with whom we share personal data provides an appropriate level of protection. However, despite these controls, no system can be guaranteed to be one hundred percent (100%) secure, and no method of transmission or storage is completely secure. To the fullest extent permitted by Applicable Data Protection Law, we shall not be liable for any unauthorised access to, loss of, misuse of, or alteration of personal data, except to the extent such liability cannot be excluded or limited under Applicable Data Protection Law. Nothing in this Policy is intended to exclude or limit liability for any matter for which liability cannot lawfully be excluded or limited.

Personal Data Breaches

Where we become aware of a personal data breach within the meaning of Article 4(12) GDPR, we will take such steps as are required under Articles 33 and 34 GDPR, including, where the breach is likely to result in a risk to the rights and freedoms of natural persons, notifying the competent supervisory authority without undue delay and, where feasible, not later than seventy-two (72) hours after becoming aware of the breach. Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, we will communicate the breach to affected data subjects without undue delay, in each case subject to and except as otherwise permitted by Articles 33 and 34 GDPR. We are not obliged to communicate a breach to data subjects where any of the conditions in Article 34(3) GDPR is met.

Third-Party Websites and Services

The Services may include links to or redirect you to third-party websites, plug-ins, applications, or other services, including social media services where you may connect with us. Third-party websites and other services may also reference or link to our websites and Services. This Policy does not apply to any personal data practices of these third-party websites, plug-ins, applications, or other services. To learn about these third parties' personal data practices, please visit their respective privacy notices.

International Transfers of Personal Data

We are incorporated outside the EEA, the United Kingdom and Switzerland, and your personal data may be transferred to, processed in, and stored in jurisdictions that may not provide a level of data protection equivalent to that provided by Applicable Data Protection Law.

Where we transfer personal data from the EEA, the United Kingdom or Switzerland to a third country (including, without limitation, the United States, the Cayman Islands, Singapore, the United Arab Emirates, and any other jurisdiction in which we, our affiliates, service providers, contractors or professional advisers operate), we rely on one or more transfer mechanisms recognised under Chapter V of GDPR, including, without limitation:

- transfers to a country, territory, sector, or international organisation in respect of which the European Commission, the United Kingdom or the Swiss Federal Council have issued an adequacy decision under Article 45 GDPR;
- transfers subject to appropriate safeguards within the meaning of Article 46 GDPR, including the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**"), the International Data Transfer Agreement and/or the UK International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner (as applicable for transfers subject to the UK GDPR), the Swiss adaptation of the EU SCCs (as applicable for transfers subject to the FADP), and binding corporate rules;
- transfers subject to a derogation set out in Article 49 GDPR, including where the transfer is necessary for the performance of a contract between you and us, where the transfer is necessary for the conclusion or performance of a contract concluded in your interest, where the transfer is necessary for the establishment, exercise or defence of legal claims, where the transfer is necessary for important reasons of public interest, or where you have explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers; and/or
- such other transfer mechanism as may be recognised under Applicable Data Protection Law from time to time.

Where we rely on EU SCCs or equivalent mechanisms, we conduct transfer impact assessments where required, and have implemented or will implement, where necessary, supplementary technical, organisational and contractual measures designed to ensure that the level of protection afforded by GDPR is not undermined. A copy of the relevant transfer mechanism (in summary form, with confidential commercial and security information redacted) is available upon written request to support@nemotrading.xyz, subject to applicable confidentiality obligations.

The jurisdictions in which personal data is processed may have data protection laws that differ from those in your jurisdiction, and personal data may be accessible to courts, law enforcement, regulators, governmental authorities or other competent authorities in those jurisdictions where permitted or required by applicable law.

Updates to This Privacy Policy

We may update this Policy from time to time. When we make changes to this Policy, we will change the date at the beginning of this Policy. If we make material changes to this Policy, we will notify individuals by email to their registered email address, by prominent posting on this website or our other platforms, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided. Your continued use of the Services after the effective date of any changes constitutes your acceptance of the updated Policy, subject to your right to withdraw any consent on which we rely.

Limitations, Reservations and Governing Law

Without prejudice to the rights expressly granted to data subjects under Applicable Data Protection Law, the following provisions apply:

- To the maximum extent permitted by law, our liability under or in connection with this Policy is limited to that which cannot be excluded or limited under Applicable Data Protection Law. Nothing in this Policy excludes or limits liability for any matter for which liability cannot lawfully be excluded or limited.
- This Policy is governed by, and shall be construed in accordance with, the laws of the Cayman Islands, without prejudice to mandatory provisions of Applicable Data Protection Law and of the law of the EEA Member State, the United Kingdom or Switzerland in which the data subject is habitually resident, and without prejudice to the courts of competent jurisdiction designated under Article 79 GDPR.
- Headings in this Policy are for convenience only and do not affect interpretation.
- References to statutes, regulations, articles and standards shall include any successor, amending, replacing, re-enacting or implementing measures from time to time in force.
- If any provision of this Policy is held to be invalid, illegal or unenforceable in any jurisdiction, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired, and the offending provision shall be deemed modified to the minimum extent necessary to render it valid, legal and enforceable.
- Where this Policy is translated into a language other than English, the English-language version shall prevail to the maximum extent permitted by Applicable Data Protection Law.
- No failure or delay by us in exercising any right or remedy under this Policy or Applicable Data Protection Law shall operate as a waiver thereof, nor shall any single or partial exercise preclude any other or further exercise.

Contact Us

If you have any questions, complaints or requests in connection with this Policy or our processing of personal data, please contact us at: support@nemotrading.xyz. We will consider and respond to your request in accordance with Applicable Data Protection Law.

You also have the right to lodge a complaint with a supervisory authority as described under Your Rights above.