Privacy Policy v4.0.1

Aligned with the T&C | Publication Date: 24 September 2026

This Privacy Policy (the "Policy") constitutes the authoritative English-language canonical version. In the event of any discrepancy between language versions, this English version prevails following its publication.

This Policy governs the collection, use, storage, disclosure, and protection of personal data in connection with the activities of Neom Triple A Information Technology LLC, operating under the brand NEOMAAA Funded.

---

§1 Controller Identification and Contact Information

1.1 **Data Controller.** The data controller within the meaning of Regulation (EU) 2016/679 (GDPR), the UK GDPR as retained and amended under the Data Protection Act 2018, UAE Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data (the 'UAE PDPL'; commonly cited as 'UAE Federal Decree-Law No. 45 of 2021'), and other applicable data-protection legislation is:

Full legal name: Neom Triple A Information Technology LLC Brand: NEOMAAA Funded Registered address: The Binary by Omniyat, Office 2114, Business Bay, Dubai, UAE Website: neomaaafunded.com

1.2 **Controller Contact Details.** For all matters relating to this Policy and the processing of personal data in connection with the Services, Participants may contact the Company through the following dedicated channels:

- Privacy enquiries, data-protection matters and exercise of data-subject rights (Privacy Contact pending DPO designation): privacy@neomaaafunded.com
- General enquiries and support: support@neomaaafunded.com

The Company aims to acknowledge all privacy-related communications promptly and will respond substantively within the timeframes prescribed by applicable law, as further detailed in §11 of this Policy.

1.3 **Relationship to T&C.** This Policy is a standalone document giving effect to the data-protection obligations set out in Chapter 29 of the Company's Terms and Conditions (the T&C, §§29.0–29.15). It must be read alongside the T&C. Where any conflict exists between this Policy and Chapter 29 of the T&C, the provisions of Chapter 29 of the T&C shall prevail. Details of the EU and UK Representatives and of the EU Data Act Representative are set out in §16 of this Policy, in accordance with §29.15 of the T&C. This Policy applies to all Participants who access or use the Services provided by NEOMAAA Funded, regardless of the jurisdiction from which they access those Services.

---

§2 Regulatory Framework

2.1 **Applicable Legal Frameworks.** The processing of personal data by Neom Triple A Information Technology LLC is carried out in accordance with the following legislation, and the Company has implemented technical and organisational measures to support compliance with each applicable framework:

(a) Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) — in respect of data subjects located in the EU/EEA. The GDPR establishes a comprehensive framework for the processing of personal data, including requirements regarding lawful bases for processing, data-subject rights, data transfers, breach notification, and accountability;

(b) UK GDPR (Regulation (EU) 2016/679 as retained and amended under the Data Protection Act 2018) — in respect of data subjects located in the United Kingdom. The UK GDPR substantially mirrors the EU GDPR in its requirements and is enforced by the Information Commissioner's Office (ICO);

(c) UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the 'UAE PDPL') and its Executive Regulations. As at the Effective Date of this Policy, the Executive Regulations to the UAE PDPL contemplated by Article 47 of the PDPL have not yet been issued by the UAE Cabinet. References in this Policy and in §6.6 of the T&C to the UAE PDPL and to "implementing regulations issued by the UAE Data Office" shall be construed accordingly. The Company will update its data-protection practices and this Policy in line with those Executive Regulations within the implementation period prescribed therein upon their issuance, and will publish a corresponding update to this Policy;

(d) The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act 2020 (CCPA/CPRA) — in respect of California residents. Additional rights specific to California residents are set out in §13 of this Policy;

(e) The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) — in respect of Canadian residents. Additional provisions applicable to Canadian residents are set out in §15 of this Policy.

2.2 **Non-Derogation Principle.** Nothing in this Policy operates to reduce any right of a data subject under any of the foregoing frameworks that is presently in force as at the Effective Date. Where any provision of this Policy is capable of more than one interpretation, it shall be interpreted in a manner that best gives effect to the applicable legal framework.

2.3 **Territorial Scope.** This Policy applies to the processing of personal data of individuals located in any jurisdiction from which they access the Services, regardless of the Company's place of incorporation, to the extent that the applicable law of that jurisdiction exercises extraterritorial effect.

---

§3 Categories of Personal Data We Collect

3.1 **Categories Collected.** We collect the following categories of personal data:

(a) **Identity data**: full name, date of birth, nationality, country of residence, government-issued identification documents (passport, national ID, driver's licence) — collected for KYC/AML compliance under §6.4 of the T&C;

(b) **Contact data**: email address, phone number, postal address, billing address;

(c) **Account data**: username, password (stored hashed and salted), account preferences, communication preferences, account status;

(d) **Payment data**: payment-instrument details (handled by third-party PSPs — see §6 of this Policy), billing history, transaction logs;

(e) **Behavioural data**: trading activity logs, dashboard interactions, IP address, device and browser characteristics, time-zone, log-in patterns;

(f) **Compliance data**: sanctions-screening results, source-of-funds declarations where required by law, fraud-prevention scoring, AML risk assessment;

(g) **Communications data**: support tickets, chat transcripts, email correspondence with the Company.

3.2 **Participant Responsibility.** Where personal data is provided by the Participant, the Participant is responsible for ensuring the information is truthful, complete, and up to date, and shall promptly notify the Company of any changes. The provision of false, inaccurate, or misleading personal data may result in suspension or termination of the Participant's account in accordance with the T&C.

3.3 **Special Category Data.** The Company does not collect special category data within the meaning of Article 9 GDPR (e.g., racial or ethnic origin, religion, biometric data for identification purposes, health data, data concerning sexual orientation) unless the Participant explicitly consents to a specific processing purpose. Identity-document images are processed for identity verification under Article 6(1)(c) GDPR (AML legal obligation) and are not treated as biometric data under Article 9 GDPR unless used for biometric identification. Where any special category data is provided by a Participant without solicitation, the Company will take reasonable steps to delete or quarantine such data promptly.

3.4 **Data Minimisation.** The Company adheres to the principle of data minimisation: only the personal data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed is collected and retained.

---

§4 Information Automatically Collected

4.1 **Automatically Collected Data.** During your visit, usage, or navigation of the Services, certain information is automatically collected by us. This information, while not revealing your specific identity (e.g. name or contact details), may include device and usage data such as IP address, browser and device specifications, operating system, language preferences, source URLs, device name, country, approximate location, usage information of our Services, and other technical details. This information is mainly utilised for ensuring the security and functioning of our Services, as well as for internal analysis and reporting purposes. Similar to other businesses, we also gather information through the use of cookies and similar technologies (see §7 of this Policy for further detail).

4.2 **Log and Usage Data.** Our servers automatically gather log and usage data when you access or utilise our Services. This data is stored in log files and may include details such as your IP address, device information, browser type and settings, and information about your activities within the Services (such as timestamps of usage, pages/files viewed, searches performed, and other actions such as feature usage), and device event information (such as system activity, error reports, and hardware configurations), depending on your interaction with us.

4.3 **Purposes of Processing Automatically Collected Data.** The data described in §4.1 and §4.2 is processed for the purposes of security monitoring, performance management, detection of anomalous trading activity and potential fraudulent behaviour, and fulfilment of legal obligations. The applicable legal bases are set out in §5 of this Policy. In particular, behavioural and log data may be used to identify patterns consistent with prohibited trading practices as defined in the T&C, including in connection with the Post-Crystallisation Compliance Review (§17.2 of the T&C).

4.4 **No Sale of Automatically Collected Data.** Automatically collected data is used solely for the operational, security, and analytical purposes described in this §4. The Company does not sell or transfer such data for purposes inconsistent with those set out in this Policy.

---

§5 Purposes of Processing and Legal Bases

5.1 The Company processes personal data on the following legal bases under Article 6(1) of the GDPR (and equivalent provisions under the UK GDPR and UAE PDPL), each tied to a specific purpose:

PURPOSE 1 — Account creation, authentication, and contract performance. Basis: Article 6(1)(b) GDPR (performance of contract). Processing is necessary to register the Participant, verify account credentials, provide access to the Services, and fulfil the Company's obligations under the Terms and Conditions. Without this processing, the Company cannot provide the Services.

PURPOSE 2 — KYC, AML, and sanctions compliance. Basis: Article 6(1)(c) GDPR (legal obligation under UAE Federal Decree-Law No. 20 of 2018 as superseded by Federal Decree-Law No. 10 of 2025; FATF Recommendations 10, 12, and 19; equivalent EU and national AML laws). Processing includes identity-document verification, sanctions-list screening, and AML risk assessment, carried out in part through KYC/AML provider Sumsub (recipient category (ii) — see §6 of this Policy). Failure to provide the necessary personal data for KYC/AML purposes will prevent the Company from onboarding the Participant.

PURPOSE 3 — Fraud prevention, platform integrity, and prohibited-trading detection. Basis: Article 6(1)(f) GDPR (legitimate interests of the Company in protecting platform integrity and the legitimate interests of other Participants and third parties), balanced against the rights and freedoms of the Participant. Processing includes monitoring of trading activity by automated systems and the conduct of the Post-Crystallisation Compliance Review (§17.2 of the T&C). The Participant's rights in relation to automated decisions are set out in §11.2(h) of this Policy.

PURPOSE 4 — Marketing communications. Basis: Article 6(1)(a) GDPR (consent obtained in accordance with §6.3(b) of the T&C). Consent may be withdrawn at any time; withdrawal does not affect the lawfulness of processing carried out prior to withdrawal. Participants who withdraw marketing consent will continue to receive transactional and service-related communications where necessary for the performance of the contract.

PURPOSE 5 — Cookies, analytics, and platform optimisation. Basis: Article 6(1)(a) GDPR (consent collected via cookie banner, where non-essential), in conjunction with the ePrivacy Directive 2002/58/EC. Strictly necessary cookies do not require consent. See §7 of this Policy for further detail on cookie categories and withdrawal of consent.

PURPOSE 6 — Legal claims, regulatory cooperation, and compliance with court orders. Basis: Article 6(1)(c) GDPR (legal obligation) and Article 6(1)(f) GDPR (legitimate interest in establishing, exercising, or defending legal claims). This includes cooperation with regulators, supervisory authorities, courts, and law-enforcement agencies where required by law, and compliance with judicial or administrative orders.

PURPOSE 7 — Customer support and dispute resolution. Basis: Article 6(1)(b) GDPR (performance of contract) and Article 6(1)(f) GDPR (legitimate interests in resolving disputes efficiently). Support interactions and correspondence are retained in accordance with the retention periods set out in §8 of this Policy.

5.2 **Legitimate Interests Assessment.** Where the Company relies on Article 6(1)(f) GDPR as a legal basis, the Company has carried out a Legitimate Interests Assessment (LIA) for each

relevant processing activity. That assessment includes an evaluation of the necessity and proportionality of the processing and a balancing test against the interests, rights, and freedoms of the data subject. Documentation of the LIA is available on request at privacy@neomaaafunded.com.

5.3 **Canadian Residents (PIPEDA).** For Canadian residents, this §5 is supplemented by PIPEDA. The Company processes personal data of Canadian residents only with their express or implied consent, except where the law permits processing without consent (fraud investigation, legal compliance, etc.). See §15 of this Policy for further detail.

---

§6 Recipients and International Transfers

6.1 **Categories of Recipients.** The Company shares personal data with the following categories of recipients. Each recipient is bound by appropriate confidentiality and data-protection obligations through written contracts, including data-processing agreements where required by applicable law:

(i) Payment service providers (PSPs) — for transaction processing, chargeback handling, and refunds;

(ii) KYC/AML and identity-verification service providers, including Sumsub — for conducting the customer identification procedure in accordance with §6.4 of the T&C;

(iii) Cloud infrastructure and content-delivery network (CDN) providers — for hosting the Services and ensuring their availability and performance;

(iv) Customer-support and helpdesk platforms — for managing and resolving Participant enquiries and support tickets;

(v) CRM, email-delivery, and marketing-automation providers — for managing communications and delivering marketing messages to Participants who have given their consent;

(vi) Analytics, observability, and platform-optimisation providers — for monitoring platform performance, detecting anomalies, and improving the Services;

(vii) Trading-platform vendors (MetaQuotes / MetaTrader 5) — for operating the MT5 trading environment made available to Participants;

(viii) Professional advisers (legal, accounting, audit, tax) — for obtaining professional advice and ensuring regulatory compliance;

(ix) Regulators, supervisory authorities, courts, and law-enforcement agencies where required by law — including in connection with legally mandated disclosures, court orders, or regulatory investigations;

(x) Successor entities in connection with a merger, acquisition, or sale of all or substantially all of the Company's assets — where personal data forms part of the assets transferred, subject to appropriate safeguards.

Participants may request a list of the specific service providers in each category at the time of the request by writing to privacy@neomaaafunded.com.

6.2 **International Transfers of Personal Data.** Cross-border transfers of personal data take place to the following identified recipients:

(i) MetaQuotes Software Corp. (Cyprus) — for MT5 platform operation;

(ii) TradeLocker / Quadcode Solutions OÜ — relevant servers in Australia and EU — for TradeLocker platform operation;

(iii) Group entities and service providers located in the United Arab Emirates.

6.3 **Transfer Mechanisms.** Each transfer is governed by Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) or applicable adequacy decisions, where required under Articles 44–49 GDPR. As a UAE-incorporated entity, the Company processes EU/EEA/UK personal data partly in the United Arab Emirates, which has not been the subject of an adequacy decision by the European Commission. The Company periodically reviews the legal frameworks applicable to international transfers and updates its transfer mechanisms as required.

6.4 **Supplementary Measures.** In the absence of an adequacy decision in respect of the UAE, the Company applies the following supplementary technical and organisational measures: encryption at rest (AES-256), encryption in transit (TLS 1.2+), access controls based on the principle of least privilege, audit logging, and contractual restrictions on onward transfer. These measures are designed to ensure that the level of protection of personal data transferred to the UAE is essentially equivalent to that guaranteed within the European Economic Area. The Company commits to completing an independent third-party technical security audit of these measures within ninety (90) calendar days of the Publication Date of this Policy and to publishing an executive summary of the audit findings (with appropriate redactions for security-sensitive details) in its Help Center upon completion.

Participants may request a copy of the Standard Contractual Clauses and a description of the supplementary measures by writing to privacy@neomaaafunded.com.

---

§7 Cookies and Tracking Technologies

7.1 **Use of Cookies.** The use of cookies and other tracking technologies (e.g. web beacons, pixels) may allow access to or storage of information on the Participant's device. This Policy does not constitute an exhaustive treatment of the Company's use of cookies: detailed information on the technologies employed, the duration of each cookie, and the options to decline certain categories of cookie is contained in the separate Cookie Notice published at neomaaafunded.com.

7.2 **Categories of Cookies.** The Company uses, in particular, the following categories of cookies:

(a) Strictly necessary cookies — required for the functioning of the Services, including authentication, security, and session management; do not require the Participant's consent;

(b) Analytical and functional cookies — used to analyse how Participants interact with and use the Services, enabling the Company to improve performance and user experience, including via Google Analytics;

(c) Marketing and advertising cookies — used to track user interactions with advertising materials and to deliver targeted advertising content, including via Google AdWords and Meta Advertising.

7.3 **Legal Basis.** For non-essential cookies (categories (b) and (c)), the legal basis is Article 6(1)(a) GDPR (the Participant's consent, obtained via cookie banner), in conjunction with the requirements of the ePrivacy Directive 2002/58/EC. Consent may be withdrawn at any time through the cookie-banner settings or in accordance with the instructions in the Cookie Notice.

7.4 **Supersession of Prior Statements.** All previously published statements indicating that the Company does not use cookies, tracking, or analytics technologies are hereby superseded by this §7 and §29.7 of the T&C. NEOMAAA Funded uses cookie technologies in accordance with this §7.

---

§8 Retention Periods

8.1 **General Principle.** The Company retains personal data only as long as necessary for the purposes for which it was collected, except where a longer period is required by law. After the applicable retention period, personal data is either deleted or irreversibly anonymised. Where deletion is not technically feasible (for example, in immutable backup snapshots), the Company securely segregates the data and restricts access until deletion becomes feasible. The Company conducts periodic reviews of the categories of personal data it holds in order to ensure that data is not retained beyond applicable retention periods.

8.2 **Specific Retention Periods.** The following retention periods apply to each category of personal data:

(a) KYC/AML records (identity documents, sanctions-screening results, source-of-funds declarations): five (5) years after the end of the business relationship with the Participant, as required by UAE Federal Decree-Law No. 20 of 2018 (as amended) and FATF Recommendation 11.

(b) Transaction records and payment data: seven (7) years from the date of the transaction, for tax, audit, and accounting purposes.

(c) Account data and trading activity logs: for the duration of the account plus three (3) years post-closure, for fraud-prevention, dispute-resolution, and legal-claim purposes.

(d) Marketing-consent records: until consent is withdrawn plus three (3) years (to demonstrate the lawfulness of historic processing under GDPR Art. 7(1)).

(e) Cookies and analytics data: maximum thirteen (13) months for analytics; session length for strictly necessary cookies.

(f) Customer-support tickets: three (3) years from closure.

(g) Backup data: rolling thirty (30) day backup cycle; full deletion of any record from backups within ninety (90) days of primary record deletion.

8.3 **Legal Obligation to Retain.** Where personal data is subject to a mandatory retention period under applicable law, the Company will retain that data for no shorter than the period required by law, regardless of any earlier request by the Participant for erasure or deletion. Participants are reminded that mandatory KYC/AML retention obligations under UAE Federal Decree-Law No. 20 of 2018 and FATF Recommendation 11 constitute a lawful basis to decline erasure requests in respect of records falling within category (a) above.

---

§9 How We Keep Your Information Safe

9.1 **Technical and Organisational Measures.** The Company has taken necessary and reasonable technical and organisational measures to secure personal data in its possession. Those measures include, without limitation: encryption at rest (AES-256), encryption in transit (TLS 1.2+), access controls based on the principle of least privilege, access-audit logging, network segmentation, regular vulnerability assessments, and regular information-security risk reviews. The Company also imposes appropriate security obligations on its service providers through written contracts.

9.2 **No Guarantee of Absolute Security.** However, the Internet and information storage technology are not foolproof, and the Company cannot guarantee that personal data will not be accessed, stolen, or altered by unauthorised third parties. While the Company strives to protect Participants' personal data, it is the Participant's responsibility to ensure the safety of the information they transmit through the Services. Participants are advised to use the Services only

in a secure environment, to use strong and unique passwords, and to notify the Company promptly of any suspected unauthorised access to their account.

9.3 **Breach Notification.** In the event of a personal-data breach likely to result in a high risk to the rights and freedoms of natural persons, the Company will notify affected Participants and, where required, the competent supervisory authority within the time limits prescribed by applicable law (including within 72 hours under Article 33 GDPR). Notifications will include, to the extent practicable, a description of the nature of the breach, the categories and approximate number of data subjects affected, the likely consequences of the breach, and the measures taken or proposed to address it.

---

§10 Minors

10.1 **Age Restriction.** The Company does not knowingly collect data from or market to individuals under 18 years of age. By using the Services, the Participant affirms that they are at least 18 years old, or that they are the parent or guardian of a minor and consent to the minor's use of the Services. The Services are not directed to individuals under the age of 18, and the Company does not knowingly enter into a contractual relationship with a minor.

10.2 **Action on Discovery of Minor's Data.** If the Company learns that personal data has been collected from a user under the age of 18 without verification of parental or guardian consent, it will delete that information and disable the associated account. If you become aware of any data the Company may have collected from a minor, please contact us immediately at support@neomaaafunded.com.

---

§11 Your Privacy Rights

11.1 **Scope.** Participants located in the EU/EEA, UK, UAE, or California have the following rights in respect of their personal data. The Company will respond to any request within one month of receipt, extendable by two further months where the request is complex or numerous (approximately ninety (90) calendar days in total), with notice to the Participant under Art. 12(3) GDPR. Where a request is received electronically, the Company will provide the response by electronic means where possible, unless the Participant requests otherwise.

11.2 **List of Rights.**

(a) **Right of access** (Art. 15 GDPR). The Participant may request confirmation of whether their personal data is being processed and obtain a copy of the data being processed, together with information about the purposes of processing, the categories of data concerned, the recipients or categories of recipients, the envisaged retention periods, the sources from which the data was collected, and the safeguards applied to any international transfers.

(b) **Right to rectification** (Art. 16 GDPR). The Participant may request the rectification of inaccurate personal data concerning them without undue delay, and, having regard to the purposes of the processing, may request the completion of incomplete personal data.

(c) **Right to erasure / 'right to be forgotten'** (Art. 17 GDPR). The Participant may request the erasure of their personal data where one of the grounds set out in Article 17 applies, unless processing is necessary for one of the reasons set out in that same Article, including compliance with the mandatory retention periods at §8.2 of this Policy (KYC/AML — 5 years, transactions — 7 years, etc.). Erasure requests will be assessed on a case-by-case basis and the Company will notify the Participant of its decision and the reasons therefor.

(d) **Right to restriction of processing** (Art. 18 GDPR). The Participant may request the restriction of processing of their personal data in the circumstances provided for in Article 18, including where the accuracy of the data is contested, where the processing is unlawful, where the Participant has objected to processing, or where the personal data is no longer needed for the purposes of processing but is required by the Participant for the establishment, exercise, or defence of legal claims.

(e) **Right to data portability** (Art. 20 GDPR). The Participant may receive their personal data in a structured, commonly used, and machine-readable format, and may request its transmission to another controller, where processing is based on consent or contract and is carried out by automated means. This right does not apply where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

(f) **Right to object** (Art. 21 GDPR). The Participant may at any time object to the processing of their personal data based on the Company's legitimate interests (Art. 6(1)(f) GDPR), including profiling on that basis. Upon receipt of such an objection, the Company will cease processing unless it demonstrates compelling legitimate grounds which override the interests, rights, and freedoms of the Participant, or unless the processing is necessary for the establishment, exercise, or defence of legal claims.

(g) **Right to withdraw consent** (Art. 7(3) GDPR). The Participant may withdraw consent to the processing of personal data at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to withdrawal. To withdraw marketing consent, use the unsubscribe link in the relevant communication or send a request to privacy@neomaaafunded.com. To withdraw cookie consent, refer to the cookie-banner settings or the Cookie Notice published at neomaaafunded.com.

(h) **Right not to be subject to solely automated decision-making** (Art. 22 GDPR). The Participant has the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. Automated decision-making for fraud prevention purposes shall be limited to detection mechanisms expressly permitted under Article 22(2)(a)–(c) GDPR, with human review available on request under Article 22(3). Where the Company uses automated systems to detect prohibited trading practices or to conduct the Post-Crystallisation Compliance Review (§17.2), decisions to suspend, terminate, claw back, or set off shall, on the Participant's written request, be reviewed by a human decision-maker before becoming final, save where the decision is required for fraud prevention or legal-compliance reasons under §1.3(a) of the T&C.

(i) **Right to lodge a complaint with a supervisory authority.** The Participant may lodge a complaint with the supervisory authority of their habitual residence. The following list is illustrative and non-exhaustive:

- Spain: Agencia Española de Protección de Datos (AEPD) — www.aepd.es
- France: Commission Nationale de l'Informatique et des Libertés (CNIL) — www.cnil.fr
- Germany: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) — www.bfdi.bund.de
- United Kingdom: Information Commissioner's Office (ICO) — www.ico.org.uk
- UAE: UAE Data Office — www.tdra.gov.ae

Where a Participant submits a complaint to a supervisory authority, they are encouraged to inform the Company simultaneously so that the Company may have the opportunity to address the matter before the supervisory authority's investigation concludes.

11.3 **Manifestly unfounded or excessive requests.** Where a request is manifestly unfounded or excessive, in particular because of its repetitive character, the Company may, in accordance with Art. 12(5) GDPR, 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 each case with notice to the Participant. The Company bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

11.4 **Verification of Identity.** To protect the security of personal data and to prevent unauthorised access, the Company may request reasonable verification of the identity of any person submitting a data-subject request before fulfilling that request.

11.5 **How to Exercise Rights.** Participants may exercise the rights set out above through either of the following channels, at their option:

(a) **Direct contact:** privacy@neomaaafunded.com.

(b) **Trust Center (Prighter PRM).** The Company provides Participants with an easy way to submit privacy-related requests such as access or erasure requests through the Privacy Rights Manager (PRM) workflow operated by its Representative, Prighter Group. To make use of data-subject rights via this channel, visit the Trust Center at https://app.prighter.com/portal/neomaaafunded.

Both channels are functionally equivalent and trigger the response timelines set out in §11.1.

---

§12 Do-Not-Track and Global Privacy Control

12.1 **Do-Not-Track (DNT).** Most web browsers and some mobile operating systems include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. There is no uniform standard for recognising and implementing DNT signals, and therefore, the Company does not currently respond to DNT signals. This position will be reviewed should a uniform technological standard emerge.

12.2 **Global Privacy Control (GPC).** The Company honours Global Privacy Control (GPC) signals as a valid opt-out request under California Consumer Privacy Act §1798.135 and the California Attorney General's guidance. Participants may exercise their right to opt out of the sale or sharing of personal information, including for cross-context behavioural advertising, under CCPA §1798.120. Where a GPC signal is detected, the Company shall treat it as an opt-out from the sale and sharing of personal information under the CCPA/CPRA and process the request accordingly.

12.3 **Limit Use of Sensitive Personal Information.** Participants also have the right to limit the use and disclosure of their sensitive personal information (including geolocation data and government-issued identifiers) to uses reasonably necessary to perform the requested Services, under CCPA §1798.121. To exercise this right, contact privacy@neomaaafunded.com with the subject line "Limit Use of Sensitive PI".

---

§13 California Residents Privacy Rights

13.1 **Applicability.** This §13 applies exclusively to California residents (United States) in accordance with the CCPA/CPRA. If you are a California resident, you are entitled to the rights set out below in addition to those set out in §11 of this Policy.

13.2 **Rights of California Residents.** If you are a California resident, you are entitled to the following rights:

(a) **Right to know.** You may request information about the categories and specific pieces of personal data that have been collected about you, the sources from which it was collected, the purposes for which it was collected, the third parties to whom it was disclosed, and the categories of those third parties. You may make such a request up to twice in any twelve-month period.

(b) **Right to deletion.** You may request the deletion of personal data collected about you by the Company, subject to the applicable exceptions under the CCPA, including where the Company is required to retain the data to comply with a legal obligation or to complete a transaction for which the personal information was collected.

(c) **Right to opt out of sale or sharing.** You may opt out of the sale or sharing of your personal data. The Company does not sell Participants' personal data to third parties within the meaning of the CCPA. However, as the Company uses digital advertising tools (Google AdWords, Meta Advertising), the transfer of data via cookies in the context of cross-context behavioural advertising may qualify as "sharing" within the meaning of the CCPA/CPRA. To opt out of such sharing, you may use the GPC mechanism described in §12.2 or adjust your preferences through the cookie-banner settings.

(d) **Right to non-discrimination.** The Company will not discriminate against you in the provision of Services for exercising any right granted under the CCPA, including by denying goods or services, charging different prices, or providing a different level of service.

13.3 **How to Submit a Request.** To exercise California privacy rights, contact support@neomaaafunded.com with the subject line "California Privacy Rights". The Company will acknowledge receipt of your request within ten (10) business days and will respond substantively within forty-five (45) calendar days, extendable by a further forty-five (45) days where necessary.

---

§14 UAE Personal Data Protection Law (PDPL)

14.1 **Applicability.** This §14 applies to the processing of personal data under UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the 'UAE PDPL') and §6.6 of the T&C. As a UAE-incorporated entity, the Company processes personal data under the UAE PDPL in addition to the other applicable frameworks set out in §2 of this Policy.

14.2 **Data-Subject Rights under UAE PDPL.** Individuals whose personal data is processed under the UAE PDPL have rights of access, rectification, erasure (subject to lawful exemptions), restriction of processing, and objection to processing, to the extent provided under the UAE PDPL. These rights are exercised in the manner set out in §11 of this Policy, subject to the following:

(a) **UAE PDPL Obligations.** The Company fulfils its obligations under the UAE PDPL, including registration with the UAE Data Office, application of standard contractual clauses for cross-border transfers of data originating from the UAE, and adoption of technical and organisational measures meeting UAE PDPL standards.

(b) **Pending Executive Regulations.** As at the Effective Date of this Policy, the Executive Regulations to the UAE PDPL have not been issued by the UAE Cabinet. As stated in §2.1(c) of this Policy, the Company will update its data-processing practices and this Policy in accordance with those Regulations following their issuance, within the implementation period prescribed therein.

(c) **Supervisory Authority.** Compliance with the UAE PDPL is supervised by the UAE Data Office. Requests and complaints may be directed to the UAE Data Office via its official portal at www.tdra.gov.ae.

---

§15 Canada (PIPEDA)

15.1 **Applicability.** This §15 applies to Canadian residents whose personal data is processed by the Company in the course of commercial activities, in accordance with the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). Where applicable provincial legislation provides a higher standard of protection, the Company will comply with such higher standard.

15.2 **PIPEDA Processing Principles.** In addition to §5 of this Policy, the Company observes the following PIPEDA accountability principles in respect of Canadian residents:

(a) **Consent.** The Company processes personal data of Canadian residents only with their express or implied consent, except where applicable law permits processing without consent (fraud investigation, legal compliance, emergency situations, etc.). Participants may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and the Company will inform the Participant of the implications of such withdrawal.

(b) **Purpose limitation.** Personal data is collected only for specified and documented purposes and is not processed in ways incompatible with those purposes. The purposes for which personal data is collected are identified before or at the time of collection.

(c) **Accuracy.** The Company takes reasonable steps to ensure that personal data is accurate, complete, and up to date for the purposes for which it is processed, and will promptly correct inaccurate data upon the Participant's request.

(d) **Supervisory authority.** Compliance with PIPEDA in Canada is overseen by the Office of the Privacy Commissioner of Canada (OPC). Canadian residents may lodge a complaint with the OPC at www.priv.gc.ca.

---

§16 EU and UK Representatives, EU Data Act Representative, and Data Protection Officer

16.1 **Privacy Representative under Article 27 GDPR and Article 27 UK-GDPR.** In accordance with Article 27 GDPR and Article 27 of the UK General Data Protection Regulation (UK-GDPR), the Company values your privacy and your rights as a data subject and has therefore appointed **Prighter Group** with its local partners as its privacy representative and your point of contact for the following regions:

- United Kingdom (UK)
- European Union (EU)

Prighter Group provides Participants with an easy way to exercise privacy-related rights (e.g. requests to access or erase personal data). To contact the Company via its Representative, Prighter, or to make use of data-subject rights, please visit the following website: https://app.prighter.com/portal/neomaaafunded.

For postal contact, the Representative may be reached at: Prighter Group, Paragon 1, Schwarzenbergplatz 4, 1030 Vienna, Austria.

16.2 **EU Data Act Representative under Article 37 Data Act ((EU) 2023/2854).** NEOM TRIPLE A INFORMATION TECHNOLOGY LLC has appointed Prighter Group as its legal representative according to Art. 37 Data Act. Prighter Group serves as the addressee for competent authorities, users and other stakeholders in the European Union on all matters related to the Data Act. To contact Prighter Group please visit the digital governance portal at https://app.prighter.com/portal/12944912068 with all information on the contact details.

16.3 **Data Protection Officer — Designation in Progress.** The formal designation of a Data Protection Officer under Article 37 GDPR is currently in progress. Pending completion of this process, all data-protection queries, data-subject access requests under Articles 15–22 GDPR, and any other matters relating to the processing of personal data may be addressed to:

- Privacy Contact: privacy@neomaaafunded.com
- Postal address: Neom Triple A Information Technology LLC, The Binary by Omniyat, Office 2114, Business Bay, Dubai, UAE

The contact details of the designated Data Protection Officer, once appointed, will be published on this page and communicated to the competent supervisory authorities in accordance with Article 37(7) GDPR.

16.4 **Reassessment.** The Company shall reassess its DPO designation arrangements at least annually and shall update this Policy if any of the mandatory triggers under Article 37(1) GDPR or Article 10 of the UAE PDPL becomes applicable, or upon completion of the ongoing designation process.

---

§17 Changes to This Policy

17.1 **Right to Amend.** The Company reserves the right to amend this Policy at any time. The current version of the Policy is always available at neomaaafunded.com. Each version of the Policy is identified by a version number and effective date in the document header. Participants are encouraged to review this Policy periodically to remain informed of the Company's data-protection practices.

17.2 **Notification of Material Changes.** Where amendments materially affect the rights of data subjects or the manner in which their personal data is processed (material changes), the Company will notify Participants in advance by:

(a) sending a notification to the email address provided upon account registration; and/or

(b) publishing a prominent notice on neomaaafunded.com.

Continued use of the Services after the effective date of any amended Policy constitutes acceptance of those amendments to the extent permitted by applicable law. Where applicable law requires explicit consent for the amendment to take effect, the Company will obtain such consent before the amended Policy is applied to the relevant processing activity.

17.3 **Archive Versions.** Previous versions of this Policy are available on request at privacy@neomaaafunded.com.

---

§18 Contact Information

18.1 **Contact Details.** For any questions, comments, or requests relating to this Policy or to the processing of personal data by the Company, you may contact us through the following channels:

Privacy enquiries, data-protection matters and exercise of data-subject rights (Privacy Contact pending DPO designation): privacy@neomaaafunded.com

General enquiries and support: support@neomaaafunded.com

Website: neomaaafunded.com

Registered address: Neom Triple A Information Technology LLC The Binary by Omniyat, Office 2114 Business Bay, Dubai, UAE

18.2 **Data-Subject Rights Requests.** Requests to exercise data-subject rights (§11 of this Policy) should be directed to privacy@neomaaafunded.com. The Company may request additional information to verify the identity of the requesting person before fulfilling a request. The Company does not charge a fee for the first copy of personal data provided in response to an access request.

18.3 **California Resident Requests.** Requests from California residents should be directed to support@neomaaafunded.com with the subject line "California Privacy Rights" (§13 of this Policy).

18.4 **Response Times.** The Company aims to acknowledge all requests within five (5) business days of receipt and to respond substantively within the timeframes prescribed by applicable law, as set out in §11 and §13 of this Policy.

This Policy supersedes all prior versions of the privacy policy published by Neom Triple A Information Technology LLC under the brand NEOMAAA Funded.

Privacy Policy v4.0.1 | Neom Triple A Information Technology LLC (NEOMAAA Funded) | Publication Date: 24 September 2026