Benevolent AI

SANCTIONS, ANTI-MONEY LAUNDERING (“AML”) AND COUNTER-TERRORIST FINANCING POLICY

1. PURPOSE

1.1 For the purpose of this sanctions, anti-money laundering and counter terrorist financing policy (the "**Policy**"), the anti-money laundering laws (the "**AML Laws**") mean applicable anti-money laundering statues of all jurisdictions in which the Group operates, including laws aimed at countering the financing of terrorism, the rules and regulations thereunder and any related or similar rules, regulations or guidelines, issued, administered or enforced by any governmental agency.

1.2 The term "**Sanctions**" means economic or financial sanctions or trade embargoes imposed, administered or enforced from time to time by (i) the United Nations, (ii) the United States, (iii) the European Union ("**EU**"), (iv) any member state of the European Union, (v) the United Kingdom, (vi) Luxembourg, (vii) any other applicable jurisdiction, or (viii) the respective governmental institutions of any of the foregoing including, without limitation, the Office of Foreign Assets Control of the US Department of the Treasury (the "**OFAC**"), the US Department of Commerce, the US Department of State and any other agency of the US government, the Luxembourg Ministry of Finance or Her Majesty's Treasury of the United Kingdom.

1.3 BenevolentAI (the "**Company**") and its subsidiaries (together, the "**Group**") recognise the significance of Sanctions and AML Laws that have been imposed and enacted by the jurisdictions in which the Group conducts business and/or to which the Group has a relevant nexus.

1.4 The Group is committed to full compliance with all applicable Sanctions (to the extent permitted under the EU Blocking Regulation (i.e. Regulation (EC) 2271/96)) and AML Laws, as well as to applicable guidelines and standards that comprise best business practices. The purpose of this Policy is to support and enable compliance by the Group and each employee within the Group (including any persons employed by, or in any other form of relationship or authority to any of the Company's subsidiaries, irrespective of the duration of employment) (an "**Employee**") with AML Laws and Sanctions, to assist law enforcement in combating money laundering, terrorism financing, and other illegal activities, and to minimise the risk of the Group being used for improper purposes.

1.5 To this end, a group-wide compliance programme comprised of risk-based policies, procedures and internal controls (the "**Compliance Programme**") is in place, which is designed to detect and prevent the use of Group companies in facilitating money laundering, terrorist financing, and other illegal activities, which are set forth in this Policy.

1.6 Failure to comply with Sanctions and AML Laws could result in civil and/or criminal penalties to the Group and/or individual Employees. As such, it is imperative that every Employee is familiar with and complies with the provisions set forth in this Policy in

order to protect the Group from being used to facilitate money laundering, terrorist financing and other crimes. The provisions of this Policy will be strictly enforced.

2. SCOPE

2.1 This Policy applies to all Employees. The Group will ensure that these persons are made aware of the applicable laws and the requirements of this Policy.

2.2 The United Kingdom, in common with many other countries (including Luxembourg), has passed legislation designed to prevent money laundering and to combat terrorism. This UK legislation, together with applicable regulations, rules and industry guidance, forms the cornerstone of this Policy and outlines the offences and penalties for failing to comply.

2.3 The requirements of UK legislation and this Policy apply to the Group globally. Individual Group companies may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdictions in which they operate. Notwithstanding this Policy, Employees are required to adhere to all applicable legislation, regulations and government approved guidance in the jurisdictions in which they operate.

3. LEGAL FRAMEWORK FOR AML AND SANCTIONS

3.1 Various jurisdictions have enacted AML Laws directed at preventing the use of the financial system for money laundering, terrorist financing, and other financial crimes and have imposed sanctions programmes that restrict the conduct of governments, entities or individuals of certain countries. The AML Laws generally exist to prevent persons involved in criminal activity—such as terrorism, drug trafficking or corruption—from committing acts to conceal or disguise the criminal origins of their money. Sanctions programmes generally seek to pressure Sanctions targets into modifying their behaviour or otherwise isolate those targets from the global economic system.

4. AML LAWS

4.1 Money laundering is generally defined as the practice of concealing or disguising the origins of proceeds derived from criminal activity, such as drug trafficking, fraud, bribery or organised crime, by creating the appearance that the proceeds are derived from a legitimate source. Money laundering usually consists of three fundamental components: placement, layering and integration. Terrorist financing is the provision of funds or "material support" for terrorist activities through illegal activity, such as drug trafficking, counterfeiting, and credit card fraud. Like other criminals, terrorists need to move funds and disguise the illegal nature or origin.

4.2 If successful, money laundering sustains a variety of criminal or terrorist activities by allowing criminals to maintain control over and use of their illicit funds, to finance additional criminal activity, and to prevent their illegal activities from being detected. The AML Laws generally exist to prevent persons involved in criminal activity from

committing acts to conceal or disguise the criminal origins of their money in order to make such funds appear as being derived from legitimate sources.

5. OVERVIEW OF LEGISLATIVE AND REGULATORY FRAMEWORK IN THE UK

5.1 The key money laundering offences, contained in the Proceeds of Crime Act 2002, include:

Acquisition, use and possession:

a) Acquiring, using or possessing criminal property.

b) The current penalty for any crime under this bracket is up to 14 years imprisonment, a fine or both.

Concealing:

a) Concealing, disguising, converting or transferring criminal property.

b) The current penalty for any crime under this bracket is up to 14 years imprisonment, a fine or both.

Arrangements:

a) Entering into an arrangement, which facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

b) The current penalty for any crime under this bracket is up to 14 years imprisonment, a fine or both.

5.2 The key terrorism related offences, contained in the Terrorism Act 2000, include:

a) Engaging in or facilitating terrorism.

b) Raising or possessing funds for a terrorist purpose, which includes clean funds intended for terrorist use, as well as the proceeds of acts of terrorism and resources of prescribed organisations.

6. SANCTIONS PROGRAMMES

6.1 Economic or financial sanctions are measures imposed by national governments and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may (i) threaten the security of the global community, or (ii) violate international norms of behaviour (e.g. human rights violations), amongst other things.

6.2 Sanctions applicable to the Group include economic or financial sanctions or trade embargoes imposed, administered or enforced from time to time by (i) the United Nations, (ii) the United States, (iii) the EU, (iv) any member state of the European Union, (v) the United Kingdom, (vi) Luxembourg or (vi) the respective governmental institutions of any of the foregoing including, without limitation, the OFAC, the US Department of Commerce, the US Department of State and any other agency of the

US government, the Luxembourg Ministry of Finance or Her Majesty's Treasury of the United Kingdom.

7. EUROPEAN UNION AND THE UNITED KINGDOM

7.1 The EU imposes an asset freeze on designated persons, entities, and bodies (along with other sanctions measures targeting certain third countries). The EU External Action Service maintains a global list of parties subject to an asset freeze where all designated parties are listed. Certain competent EU Member State government agencies may also maintain their own asset freeze lists (including the EU designated parties). The EU and its Member States also impose general export controls on military and dual-use items, including when such items are brokered by EU parties in third countries.

7.2 The UK formerly implemented EU Sanctions while it was an EU Member State, and during the implementation of the withdrawal agreement period (ending on 31 December 2020). Since 1 January 2021, the UK has operated an independent sanctions regime, in which UK Sanctions are implemented through domestic regulations enacted pursuant to the Sanctions and Anti-Money Laundering Act 2018 ("**SAMLA**"). The UK's financial sanctions are overseen and enforced by the Office of Financial Sanctions Implementation ("**OFSI**") within Her Majesty's Treasury.

8. UNITED STATES

8.1 Sanctions programs impose a range of financial or trading restrictions, such as freezes on the assets of designated individuals and entities, bans on financing of certain state-owned or other enterprises, prohibitions or restrictions on certain types of trade along with the supply of certain related technical, financial and other assistance.

8.2 In the US, the OFAC administers and enforces US-based economic and trade sanctions programs ("**OFAC Sanctions Programs**"), which are based on US foreign policy and national security goals, as well as on United Nations and other international mandates. Additionally, OFAC publishes lists of individuals, groups and entities, such as terrorists and narcotics traffickers, which are the target of the OFAC Sanctions Programs. These include: the Specially Designated Nationals ("**SDNs**") and Blocked Persons List ("**SDN List**"), the Foreign Sanctions Evaders List ("**FSE List**"), and the Sectoral Sanctions Identifications List ("**SSI List**") (collectively, "**OFAC Lists**"). The US also maintains "secondary sanctions" programs that allow the US to impose sanctions on any non-US entity that engages in targeted activities, even if those activities do not violate US law or the laws of the non-US person's home jurisdiction. OFAC also has in place a series of comprehensive embargoes that prohibit dealings involving: (i) Cuba; (ii) Iran; (iii) North Korea; (iv) Syria; (v) Russia; and (vi) the Crimea/Sevastopol region of Ukraine (the "**Sanctioned Territories**").

8.3 The Group generally applies the OFAC Sanctions Programs as if it is a US person. This is done for a number of reasons, including management of business and reputational risk, and because the OFAC Sanctions Programs apply to non-US

companies in many cases, such as, for example, if a transaction that takes place outside the United States between non-US persons calls for payment in US dollars.

9. LUXEMBOURG

9.1 In line with the Luxembourg law of 19 December 2020 on the implementation of restrictive measures in financial matters (the "**Law on restrictive measures**"), Luxembourg implements the restrictive measures in financial matters adopted by the United Nations Security Council and the European Union by grand-ducal regulations.

9.2 Without prejudice to more severe penalties provided for, where applicable, by other legal provisions, failure to comply with the restrictive measures adopted pursuant to the Law on restrictive measures is punished by imprisonment of 8 days to 5 years and/or a fine between EUR 12,500 and EUR 5,000,000. Where the offence has resulted in substantial financial gain, the fine may be increased to four times the amount of the offence.

10. RESPONSIBILITY FOR COMPLIANCE WITH THIS POLICY

10.1 The responsibility of ensuring compliance with this Policy and ensuring effective controls to prevent money laundering and terrorist activity vests with all Employees. Notwithstanding, there is a varying level of responsibility across the organisation to deter money laundering and terrorist activity depending on the performance of a certain role or function within the Group. Below is a non-exhaustive list of responsibilities within the Group that vest within a role or function.

10.2 If despite having received training and completed the relevant competency requirements within the Group, there is any doubt in relation to the responsibilities under this Policy and the guidance issued from time to time, the relevant Employee or function must consult the Compliance Manager.

Audit Committee Responsibility

a) To review the adequacy and effectiveness of the Group's anti-money laundering systems and controls on an annual basis and review regular reports from senior management and the adequacy and effectiveness of the Group's anti-money laundering systems and controls.

Senior Management Responsibility

a) To establish effective policies and guidance and be responsible for monitoring their effectiveness.

b) To ensure employees are adequately trained in relation to their obligations under this Policy and ensuring that employees show an understanding and competence in relation to their duties to deter and prevent money laundering and terrorist activity.

Accounts Team Responsibility

a) To monitor any payments, which are received directly into the accounts department, keeping senior management and the Compliance Manager informed as appropriate.

Customer Facing Roles and other Skilled and Technical Roles (ST) Responsibility

a) To read, understand and follow the requirements of this Policy ensuring any reportable events, and any other suspicions of money laundering/terrorist financing are immediately referred to the Compliance Manager.

b) To attend training activities relevant to the requirements of this Policy and procedures.

Team Leaders & Managers Responsibility

a) To ensure their team members are aware of their responsibilities and follow this Policy and procedures.

b) To ensure they maintain effective governance and controls of this Policy.

Internal Audit Team Responsibility

a) To conduct periodic (risk based) internal audits of compliance with this Policy and procedures.

Legal Team Responsibility

a) Maintenance and review of this Policy.

b) Monitor new legislation on money laundering.

c) Conducting sanctions screening.

d) Advise on technical requirements to ensure compliance with laws, regulations, and guidance in connection with the prevention of money laundering and terrorist activity.

11. AML AND SANCTIONS COMPLIANCE PROGRAMME

11.1 To promote compliance with all applicable AML and sanctions laws, the Company has adopted and will enforce this AML and Sanctions Compliance Program which is reasonably designed to prevent the Group from being used to facilitate money laundering or other illegal activities and cause the Group to comply with applicable AML and sanctions laws. The provisions of the AML and Sanctions Compliance Program are discussed in the sections below.

12. RISK ASSESSMENT

12.1 Each year the Audit Committee undertakes a risk assessment in relation to anti-money laundering and counter terrorist financing to assess the Group's risk, in order to assess, amongst other things, whether there have been any changes to the nature of the risks

which the Group faces and whether there should be any changes made to this Policy and the procedures set out herein.

13. TRAINING AND COMPLIANCE

13.1 One of the most important controls over the prevention and detection of money laundering and terrorist financing is to have Employees who are alert to the risks and are trained in identifying potential suspicious transactions.

13.2 All Employees are responsible for reading and having access to the Policy. Periodic training for anti-money laundering will be provided.

14. MONITORING, DETECTION AND REPORTING OF SUSPICIOUS ACTIVITY

14.1 US and UK AML laws generally provide for the monitoring, detection, and in appropriate circumstances, the reporting of suspicious transactions to the relevant authorities. Accordingly, the Group has implemented appropriate and risk-based procedures that provide for the identification and scrutiny of transactions that may be related to money laundering, such as, for example, unusual patterns of transactions, transactions that do not match the customer's profile, transactions involving suspicious countries, or transactions that have no apparent economic or lawful purpose.

14.2 In the event that an Employee becomes aware of facts and circumstances that may indicate potential money laundering, terrorist financing or other illicit activities, these matters must be promptly reported to the Compliance Manager. Employees should immediately (and no later than 24 hours) report any "red flags" relating to possible violations to the Compliance Manager, who will determine what actions should be taken by the Group.

14.3 Such red flags include, but are not limited to, the following:

(a) Notification by computerised screening of a customer in relation to countries, persons or entities that are the target of applicable sanctions administered and enforced by the US Government (including the OFAC Sanctions Programs and OFAC Lists, defined above) or another competent government agency or by the EU or the UK;

(b) Notification by computerised screening of a customer in relation to financial dealings in countries either identified as being non-cooperative with international efforts against money laundering (e.g., by the Financial Action Task Force or against whom the US Treasury Department has issued an advisory);

(c) Refusal or reluctance to disclose or provide documentation concerning identity, nature of business, nature and source of assets;

(d) Providing false, misleading or substantially incorrect information;

(e) Refusal or reluctance to identify a principal or beneficial owner of a customer (e.g., a shell company or agent, acting on behalf of an undisclosed third party);

(f) Engaging in transactions that appear to have been structured so as to avoid government reporting requirements;

(g) Concern about compliance with government reporting requirements;

(h) Lack of concern regarding risks or other transaction costs;

(i) The customer or service provider wishes to engage in a transaction that lacks business sense, economic substance or apparent investment strategy;

(j) Assets well beyond the customer's or party's known income or resources;

(k) Request that funds be transferred to a third party, such as an unrelated party or to a jurisdiction other than the one in which the party is located, particularly if located in an 'off shore' bank secrecy or tax haven;

(l) The customer or party, or any person associated with the customer or party, is or has been the subject of any known formal or informal allegations (including in the reputable media) regarding possible criminal, civil or regulatory violations or infractions;

(m) The number of employees is unusually low taking into account the scope of the business;

(n) The customer or party possesses assets or is acquiring assets (i.e., boats, luxury cars, etc.) which do not relate to its business;

(o) Constituent documents of the customer or party do not reflect the activities performed, although legally required;

(p) The customer or party makes payments which are disproportionate to its financial capacity;

(q) The party's invoices show gaps or missing information (e.g., missing VAT-number, account number, invoice number, or address or date);

(r) Funds are received from or the customer or party requests that funds are distributed to unrelated third parties or bank accounts in countries other than the customer's country of origin or residence; or

(s) Funds are received from or the customer or party requests that funds are distributed to unrelated third parties or bank accounts in countries where drug trafficking or money laundering is known to occur or to other high risk countries or jurisdictions or financial secrecy haven countries.

14.4 All Employees must report promptly to the Compliance Manager when they become aware of facts and circumstances that may indicate potential money laundering, terrorist financing or other illegal activity. The Compliance Manager will consider the circumstances and decide on the appropriate next steps.

14.5 Reports by an Employee to the Compliance Manager will be kept confidential and the Employee will not be subject to any retaliation for any reports made in good faith. Employees must not disclose such reports, or information pertaining to a violation of sanctions programs or AML laws which has been included in such reports, to any other person (including the person who is the subject of the report), except as may be required by law or regulation or in connection with an internal review by the Group. The

Compliance Manager, after consultation with external counsel, will advise the Employee if such an exception applies.

15. PROHIBITED TRANSACTIONS

15.1 The Group and its Employees will deploy standard customer / client on-boarding procedures for the jurisdictions in which the Group operates as of the date of this Policy. This may be subject to update in light of future openings in other jurisdictions.

15.2 When the Group enters into a commercial relationship with a new business partner, it should ensure that it verifies that the new business partner is not one of the counterparties with whom the Group may not transact business ("**Prohibited Counterparties**"), being:

(a) any person who is designated as a subject of Sanctions;

(b) any person who is resident in, located in, operating from, or incorporated under the laws of, a Sanctioned Territory;

(c) any legal person owned (by 50% or more) or controlled by one or more person who is designated as a subject of Sanctions;

(d) any person whose name appears on any list of known or suspected terrorists or terrorist organisations issued by the relevant authorities; and

(e) such other lists of prohibited persons and entities as may be mandated by applicable law or regulation.

15.3 The Compliance Manager will be responsible for (i) determining and updating the Group on any directives which may be issued with respect to any applicable lists issued by the US government and any maintained on OFAC's website or website of The Financial Action Task Force which lays down international AML and counter-terrorism financing standards, sanctions imposed by Her Majesty's Treasury and/or European Union sanctions adopted by the Council of the European Union; (ii) monitoring the website of the US Department of the Treasury's Financial Crimes Enforcement Network ("**FinCEN**") for information on foreign jurisdictions, institutions, classes of transactions, or types of accounts that have been designated as a primary money laundering concern and any special measures that have been imposed pursuant to Section 311 of the USA Patriot Act or any other applicable laws and any other sanctions imposed by Her Majesty's Treasury and/or adopted by the Council of the European Union. The Group will also follow all US directives issued in connection with any list of known or suspected terrorist or terrorist organisation designated by the Treasury Department. The Group will not establish any relationships with Prohibited Counterparties nor engage in any transactions with Prohibited Counterparties.

15.4 To the extent the sanctions programs of other countries or regions apply to the Group's business activities, the Compliance Manager will be responsible for performing

activities corresponding to the steps outlined above for those applicable jurisdictions as well.

16. POLITICALLY EXPOSED PERSONS

16.1 On occasions, the Group may identify someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person (a "**PEP**"). A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Upon identification of a PEP, enhanced due diligence is required in order to validate the source of any monies to be received by the Group, or the destination of any monies to be given by the Group. The Compliance Manager will determine what enhanced due diligence is required in these circumstances.

17. HIGH RISK COUNTRIES

17.1 Generally, criminals tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering controls and then move funds through stable financial systems.

17.2 Where transactions originate from a high-risk country, enhanced due diligence and/or approval from the senior management and/or Compliance Manager may be required depending on the level of risk posed by the transaction. The Compliance Manager will determine what enhanced due diligence and whether approval is required in these circumstances. If there is any doubt in relation to whether a transaction originated from a high-risk country, the relevant Employee or function must consult the Compliance Manager for guidance.

18. CONSEQUENCES OF NON-COMPLIANCE

18.1 All Employees have a strict duty to comply with this Policy and the AML Laws and Sanctions referred to in this Policy.

18.2 Failure to comply with this Policy may constitute a disciplinary offence and/or a criminal offence.

19. KEEPING RECORDS

19.1 The Group is required to keep full records in order to monitor and manage our money laundering risks in the business. It must therefore ensure that adequate systems and controls are in place in keeping records of the customer and the transaction(s) involved.

19.2 The Group shall develop systems and controls to retain such records for 7 years after the business relationship has ended.

Approved by the Board on 15 December 2023.