Benevolent AI

DATA PROTECTION POLICY STATEMENT

1. Introduction

1.1 Background to the EU and UK General Data Protection Regulation (collectively, "GDPR")

Regulation (EU) 2016/679 ("**EU GDPR**") and the post-Brexit UK General Data Protection Regulation 2016 ("**UK GDPR**") replaced the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, where possible, that it is processed lawfully, fairly, and transparently.

Accordingly, the United Kingdom's government updated the Data Protection Act 1998 to meet the tenets set out in the GDPR. The Data Protection Act 2018 ("**DPA 2018**") controls how personal information is used by organisations, businesses, or the government. The DPA 2018, UK GDPR, and EU GDPR apply throughout this policy statement.

1.2 Definitions used in this Policy (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the UK GDPR applies to all controllers that are established in the UK who process the Personal Data of Data Subjects, in the context of that establishment. It also applies to controllers/processors outside of the UK that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are residents of the UK. The EU GDPR applies to all controllers that are established in the EU who process the Personal Data of Data Subjects, in the context of that establishment. It also applies to controllers/processors outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are residents of the EU.

1.3 Article 4 definitions

Establishment – under the UK GDPR, the main establishment of the controller in the UK will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the UK will be its main administrative centre. If a controller is based outside the UK, it will have to appoint a representative in the jurisdiction in which the controller operates within the UK to act on behalf of the controller and deal with the supervisory authority. BenevolentAI's head office is 4 - 8 Maple Street, London W1T 5HD, United Kingdom.

Under the EU GDPR, the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its main administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates within the

EU to act on behalf of the controller and deal with the supervisory authority. BenevolentAI is a Luxembourg registered public limited company ("*société anonyme*") with its registered office at 9 rue de Bitbourg, L-1273 Luxembourg, Grand Duchy of Luxembourg. For all Group entities processing personal data within the scope of the EU GDPR, the relevant entities shall appoint BenevolentAI as their EU representative.

Personal data – any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by BenevolentAI Group.

Processing – any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on BenevolentAI Group to report personal data breaches to the supervisory authority (the ICO – Information Commissioner's Office in the UK, or the Commission Nationale pour la Protection des Données – CNPD in Luxembourg) where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a

statement or by clear affirmative action, signifies agreement to the processing of personal data.

Pseudonymisation – means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Data concerning health – means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Representative – means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under the GDPR.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this has been lowered to 13 in the UK. The processing of the personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility for the child. In the UK, anyone from the age of 13 is regarded as an adult under the UK GDPR/DPA 2018.

Third-party – a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.

1.4 Article 25 definitions

Data Protection by Design - is a framework that ensures we consider privacy, data protection, and security issues right from the start of any system, service, product, project, or process and then throughout the lifecycle.

Security by Design - an approach that integrates risk-appropriate security controls into all aspects of the design, development, implementation, operation, and decommissioning of IT information systems and business processes

Privacy and Security by Default - an approach that implements appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific, identified purpose of the processing are processed.

2. Policy statement

2.1 BenevolentAI (the "**Company**" and, together with its subsidiaries, the "**BenevolentAI Group**", "**we**", "**us**" and "**our**") is committed to compliance with

all relevant EU and UK laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information the Group collects and processes in accordance with the EU GDPR, the UK GDPR and DPA 2018.

2.2 Compliance with the DPA 2018, the UK GDPR, and the EU GDPR is described by this Policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

2.3 The DPA 2018 / UK GDPR / EU GDPR and this Policy apply to all of BenevolentAI Group's personal data processing functions, including those performed on customers', clients', employees', patients', suppliers', partners', and collaborators' personal data, and any other personal data processed from any other sources by BenevolentAI Group.

2.4 BenevolentAI Group established objectives for data protection and privacy, which forms BenevolentAI Group's **Data Protection and Privacy Compliance Programme.**

2.5 The Data Protection Officer is responsible for annually reviewing the records of processing activities (Article 30) in light of any changes to BenevolentAI Group's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments (DPIA). The register is continuously updated and will be available at the supervisory authority's request.

2.6 This policy applies to all colleagues, suppliers, partners, collaborators, and processors of BenevolentAI Group inclusive of all outsourced consultants and contractors. Any breach of the DPA 2018 / UK GDPR / EU GDPR or the personal information management system (PIMS) will be dealt with under BenevolentAI Group's disciplinary policy and may also be a criminal offense, in which case the matter will be reported to the appropriate authorities without any delays.

2.7 Partners and any third parties working with or for BenevolentAI Group, and who have or may have access to personal data, will be expected to have read, understood, and comply with this policy. No third party may access personal data held by BenevolentAI Group without having first entered into a data confidentiality agreement that imposes on the third-party obligations no less onerous than those to which BenevolentAI Group is committed, and which gives BenevolentAI Group the right to audit compliance with the agreement (where applicable).

2.8 To support compliance with the DPA 2018 / UK GDPR / EU GDPR, the executive management team approves and supports the development, implementation, maintenance, and continual improvement of a documented personal information management system (PIMS) for BenevolentAI Group.

2.9 All colleagues, contractors, suppliers, consultants, partners, and processors of BenevolentAI Group are expected to comply with this Policy and with the PIMS that implements/informs this Policy. All colleagues, and certain external parties, will receive appropriate training where applicable. The consequences of breaching this policy are set out in BenevolentAI Group's disciplinary policy and in contracts and agreements with third parties (as applicable).

2.10 In determining the scope for compliance with this policy (covering all of the Personally Identifiable Information (PII), pseudonymised datasets, patient-level data, and any other personal information that BenevolentAI Group holds or shares with external organisations such as suppliers, cloud providers, processors, collaborators, partners, or for third countries transfers), the DPA 2018 / UK GDPR / EU GDPR and BenevolentAI Group considers:

- any external and internal issues that are relevant to the purpose of, and that affect its ability to achieve the intended outcomes of its PIMS;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- organisational objectives and obligations which evolve from time to time;
- the organisations acceptable level of risk as informed by our risk appetite; and
- any applicable statutory, regulatory, legal, or contractual obligations.

BenevolentAI Group's objectives for compliance with the DPA 2018 / UK GDPR / EU GDPR and PIMS:

- are consistent with this policy
- are measurable
- take into account data protection requirements, the results from risk assessments, and risk treatments
- are monitored in line with the Group's monitoring procedure
- are communicated in line with the Group's communication procedure
- are updated as appropriate in line with the Group's continual improvement procedure

In order to achieve these objectives, BenevolentAI Group determines:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated and measured

3. Responsibilities and Roles

3.1 BenevolentAI is a data controller under the DPA 2018, the UK GDPR, and the EU GDPR.

3.2 The management team and all colleagues in managerial and supervisory roles throughout BenevolentAI Group are responsible for encouraging good

information handling practices both internally and externally as part of their corporate governance responsibility and accountability.

3.3 The Data Protection Officer's job description and responsibilities, a role specified in the UK GDPR and the EU GDPR, is accountable to the board of directors of the Company, via an assigned line manager for the management of personal data within BenevolentAI Group and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

(a) development, implementation, and maintenance of the DPA 2018 / UK GDPR / EU GDPR as required by this policy; and

(b) actively supporting security and risk management in relation to compliance with this Policy.

3.4 The Data Protection Officer, who the executive management team considers to be suitably qualified and experienced, has been appointed to take responsibility for BenevolentAI Group's compliance with this Policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that BenevolentAI Group complies with the tenets of DPA 2018 / UK GDPR / EU GDPR and monitoring personal data processing activities that take place throughout the organisation.

3.5 The Data Protection Officer has specific responsibilities with respect to procedures such as the Data Subject Access Request Procedure and is the first point of call for colleagues seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all colleagues of BenevolentAI Group who process personal data.

3.7 BenevolentAI Group's Training Policy sets out specific training and awareness requirements in relation to specific roles and colleagues of BenevolentAI Group generally.

3.8 Colleagues are responsible for ensuring that any personal data about them which are supplied to BenevolentAI Group is accurate and up to date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in chapter 2, part 2 of the DPA 2018, Article 5 of the UK GDPR, and Article 5 of the EU GDPR. BenevolentAI Group's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly, and transparently

Lawful – BenevolentAI Group identifies lawful basis before processing personal data. These are often referred to as the "conditions for processing", for example, contractual or legal.

Fairly – in order for processing to be fair, BenevolentAI Group (the data controller) has made certain information available to the data subjects as practicable on our privacy notice. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The DPA 2018, the UK GDPR, and the EU GDPR increased the requirements on what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the DPA 2018, the UK GDPR, and the EU GDPR include rules on giving privacy information to data subjects in Articles 12, 13, and 14 of the UK GDPR and in Articles 12, 13, and 14 of the EU GDPR. These are detailed and specific, placing emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. BenevolentAI Group's Privacy Notice is recorded and is publicly available here.

The specific information that must be provided to the data subject must, as a minimum, include:

(a) the identity and the contact details of the controller;

(b) the contact details of the **Data Protection Officer;**

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the period for which the personal data will be stored;

(e) the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

(f) the categories of personal data concerned;

(g) the recipients or categories of recipients of the personal data;

(h) where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data; and

(i) any further information necessary to guarantee fair processing.

4.2 **Personal data can only be collected for specific, explicit, and legitimate purposes (Purpose Limitation)**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the data subjects, data suppliers, or the supervisory authority as part of BenevolentAI Group's record of processing activities. Please see the Privacy Procedure which sets out the relevant procedures.

4.3 **Personal data must be adequate, relevant, and limited to what is necessary for processing (Data Minimisation)**

(a) The Data Protection Officer is responsible for working with the Data Manager to ensure that BenevolentAI Group does not collect information that is not strictly necessary for the purpose for which it is obtained.

(b) All data collection forms (electronic, digital, paper-based, or any other usable formats used), including data collection requirements in new information systems, must include a fair processing statement or link to the privacy statement as recommended and approved by the Data Protection Officer.

(c) The Data Protection Officer will ensure that, on an annual basis, all data collection methods are reviewed through an internal audit process to ensure that collected data continues to be adequate, relevant, and not excessive (Data Protection Impact Assessment Procedure and Data Protection Impact Assessment Tool are used as a guide).

4.4 **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay (Accuracy)**

(a) Data that is stored by BenevolentAI Group must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

(b) The Data Protection Officer is responsible for ensuring that all colleagues are trained in the importance of collecting and maintaining accurate data.

(c) It is also the responsibility of the data subjects to ensure that the data held by BenevolentAI Group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission where applicable.

(d) Colleagues and all external stakeholders are required to notify BenevolentAI Group of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of BenevolentAI Group to ensure that any notification regarding change of circumstances is recorded and timely acted upon.

(e) The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change, and any other relevant factors.

(f) On an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by BenevolentAI Group, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Retention Procedure.

(g) The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (the Data Subject Access Request Procedure is followed). Access requests can be extended to a further two months depending on complexity. If BenevolentAI Group decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain the reasons for such a decision and inform them of their right to complain to the supervisory authority and seek judicial remedy.

(h) The Data Protection Officer is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned, and for passing any correction to the personal data to the third party where this is required.

4.5 **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing (Storage Limitation)**

(a) Where personal data is retained beyond the pre-agreed processing date, it will be minimised and stored in a BenevolentAI Group's encrypted system in order to protect the identity of the data subject in the event of a data breach.

(b) Personal data will be retained in line with appropriate timelines and, once its retention date is passed, it will be securely destroyed as set out in this procedure.

(c) The Data Protection Officer must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be explicit.

4.6 **Personal data must be processed in a manner that ensures the appropriate security (Integrity and Confidentiality)**

The Data Protection Officer will carry out a risk assessment considering all the circumstances of BenevolentAI Group's controlling operations.

In determining appropriateness, the Data Protection Officer shall also consider the extent of damage or loss that might be caused to individuals (e.g. colleagues, collaborators, partners, investors, or suppliers) if a security breach occurs, the effect of any security breach on BenevolentAI Group itself, and any reputational damage including the possible loss of trust.

When assessing appropriate technical measures, the Data Protection Officer together with the IT and Information Security Team will consider the following (see the Information Security Policy for further details):

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary colleagues;
- Encryption of all devices that leave the organisation's premises such as laptops;
- Security of local and wide area networks;
- Privacy-enhancing technologies such as encryption and anonymisation where applicable;
- Identifying appropriate international security standards relevant to BenevolentAI Group business operations.

When assessing appropriate organisational measures, the Data Protection Officer will consider the following:

- the appropriate training levels throughout BenevolentAI Group;
- measures that consider the reliability of colleagues (such as good references);
- the inclusion of data protection in employment contracts;
- identification of disciplinary action measures for data breaches;
- monitoring of colleagues for compliance with relevant security standards;
- physical access controls to electronic and paper-based records;
- adoption of a clear desk policy;
- storing of paper-based data in lockable fire-proof cabinets;
- restricting the use of portable electronic devices outside of the workplace;
- implementing the bring your own device (BYOD) policy;
- adopting clear rules about passwords;
- making regular backups of personal data;
- the imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the UK or EEA; and
- maintaining a procedure for the decryption of encrypted material, where encrypted data is stored in a third country and where the processor should not have control over the decryption key.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed by BenevolentAI Group.

BenevolentAI Group's compliance with this principle is in accordance with the Information Security Management System (ISMS), which aligns with ISO/IEC 27001 and the Information Security Policy.

4.7 **The controller must be able to demonstrate compliance with the DPA 2018 and UK GDPR's / EU GDPR's other principles (Accountability)**

The DPA 2018 / UK GDPR / EU GDPR includes provisions that promote accountability and governance. These complement the regulations' transparency requirements. The accountability principle in Article 5(2) of the UK GDPR and Article 5(2) of the EU GDPR requires BenevolentAI to demonstrate compliance with the principles and states explicitly that this is a core responsibility.

BenevolentAI Group will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, timely DPIAs, breach notification procedures, and incident response plans.

5. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

(a) To make subject access requests regarding the nature of information held and to whom it has been disclosed.

(b) To prevent processing likely to cause damage or distress.

(c) To prevent processing for purposes of direct marketing.

(d) To be informed about the mechanics of automated decision-making processes that will significantly affect them.

(e) To not have significant decisions that will affect them taken solely by an automated process.

(f) To sue for compensation if they suffer damage by any contravention of the DPA 2018 and the UK GDPR or the EU GDPR.

(g) To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data where applicable.

(h) To request the supervisory authority to assess whether any provision of the DPA 2018 and UK GDPR or EU GDPR has been contravened.

(i) To have personal data provided to them in a structured, commonly used, and machine-readable format and the right to have such data transmitted to another controller.

(j) To object to any automated profiling that is occurring without consent.

5.2 BenevolentAI Group ensures that data subjects may exercise these rights:

(a) Data subjects may make data access requests as described in the Data Subject Access Request Procedure. This procedure also describes how BenevolentAI Group will ensure that its response to the data access request complies with the requirements of the DPA 2018 and UK GDPR or EU GDPR.

(b) Data subjects have the right to complain to the BenevolentAI Group relating to the processing of their personal data. The handling of a request from a data subject and appeals from a data subject on how complaints will be handled are outlined in the BenevolentAI Group's Complaints Procedure.

6. Appointment of data processors

6.1 The BenevolentAI Group shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures such that the Processing meets the requirements of the GDPR and ensures the protection of the rights of the data subject.

6.2 When the BenevolentAI Group engages the services of a processor to Process Personal Data on its behalf and the processor is a third party, BenevolentAI Group shall select a data processor that provides appropriate assurances as to the level of security it shall employ in respect of the Personal Data to be processed.

6.3 BenevolentAI Group shall ensure that a contract is entered into with third-party processors that address relevant requirements of the GDPR; provide appropriate detail on how those requirements are satisfied in practice; and as a minimum require that the processor shall:

(a) act only on instructions from the controller;

(b) impose a duty of confidentiality on relevant staff;

(c) implement security measures;

(d) subcontract only with the controller's prior permission, and by written contract with the subcontractor;

(e) make arrangements to enable the controller to fulfill the rights of data subjects (see above);

(f) assist the controller in complying with its obligations regarding data security and consultation with supervisory authorities;

(g) return all relevant Personal Data to the controller after the end of the Processing and not process the relevant Personal Data further; and

(h) make available to the controller and the supervisory authority all necessary information regarding the processor's data Processing activities.

7. Record of processing

7.1 The Group shall maintain a record of processing activity under its responsibility and shall make the record available to the supervisory authority on request.

7.2 The DPO shall be responsible for producing and maintaining the record of processing. It shall be reviewed and updated at least annually no more than two months following the internal audit.

7.3 The record shall contain:

(a) the name and contact details of the legal entity that is the controller or processor for the relevant Personal Data (and the contact details of the DPO responsible for such Personal Data);

(b) the purposes and legal basis of Processing, a description of the categories of data subjects for the Personal Data;

(c) the categories of recipients to whom Personal Data has been or may be disclosed (identifying which, if any, are established outside the European Union or the UK, or for which the data transfer involves an export of Personal Data outside the European Union or the UK);

(d) where possible, the data retention rules applicable to the relevant Personal Data; and

(e) where possible, a general description of the technical and organisational measures applicable to the relevant Personal Data.

7.4 Any new IT systems, databases, or new Processing activities must be communicated to the DPO so they can be included in the record of processing.

8. Consent

8.1 BenevolentAI Group understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed, and unambiguous indication of the data subject's wishes that, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time where applicable.

8.2 BenevolentAI Group further understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified

their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Any consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

8.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. BenevolentAI Group can demonstrate that consent was obtained for the processing operation (where applicable).

8.4 For sensitive personal data, explicit written consent (Consent Procedure) of data subjects will be obtained by BenevolentAI Group unless an alternative legitimate basis for processing exists.

8.5 Where applicable, consent to process personal and sensitive data may be obtained routinely by BenevolentAI Group using standard consent documents (e.g. Google form) when a new client signs a contract, or during an event or induction process.

8.6 Where BenevolentAI Group decides to provide services to children, parental or custodial authorisation will be obtained. This requirement applies to children under the age of 13 in the UK and may apply to children under the age up to 16 in some EU Member States.

9. Security of data

9.1 All colleagues are responsible for ensuring that any personal data that BenevolentAI Group holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by BenevolentAI Group to receive that information and has entered into a confidentiality agreement.

9.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

9.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised colleagues of BenevolentAI Group. All colleagues are required to read and attest to understanding the Acceptable Use Policy before they are given access to organisational information of any sort, which details rules on screen time-outs.

9.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving accordingly.

9.5 Personal data may only be deleted or disposed of in line with set timelines. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed or securely purged as required. Please also refer to the Information Security Policy.

9.6 Processing of personal data off-site presents a potentially greater risk of loss, theft, or damage to personal data. All colleagues must be specifically authorised to process data off-site in line with remote and flexible working procedures.

10. Disclosure of data

10.1 BenevolentAI Group ensures that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All colleagues are trained to always exercise caution when asked to disclose personal data held on another individual to a third party and channel such request to the Data Protection Officer to ascertain if the request aligns with the permissible situations for disclosure such as:

- to safeguard national security;
- the prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety, and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, (this refers to life and death situations).
- and whether or not the disclosure of such information is relevant to, and necessary for, the conduct of BenevolentAI Group's business operations.

10.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

11. Retention and disposal of data

11.1 BenevolentAI Group shall not keep personal data in a form that permits identification of data subjects for a longer period than necessary, in relation to the purpose(s) for which the data was originally collected.

11.2 BenevolentAI Group may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

11.3 The retention period for each category of personal data is set out along with the criteria used to determine this period including any statutory obligations BenevolentAI Group has to retain the data.

11.4 BenevolentAI Group's data retention and data disposal procedures will apply in all cases.

11.5 Personal data must be disposed of securely in accordance with the sixth principle of the UK GDPR and EU GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

12. Data transfers

12.1 All exports of data from the UK and within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the DPA 2018, the UK GDPR, and the EU GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the UK (respectively EEA) is prohibited by the UK GDPR (respectively EU GDPR) unless one or more of the specified safeguards, or exceptions, apply:

(a) **An adequacy decision**

The UK (respectively EU Commission) can and does assess third countries, a territory, and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

Countries that currently satisfy the adequacy requirements under the UK GDPR are listed in the ICO's International transfer after the UK exit from the EU. Countries for which the EU Commission has adopted an adequacy decision are listed on this website.

Assessment of adequacy by the data controller

In assessing adequacy, BenevolentAI Group (which is a UK-based exporting controller) will take into account the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken regarding the data in the overseas location.

(c) **Binding corporate rules**

BenevolentAI Group may adopt approved binding corporate rules for the transfer of data outside the UK/EEA. This requires submission to the relevant supervisory authority (ICO or CNPD) for approval of the rules that BenevolentAI Group is seeking to rely upon.

(d) **Exceptions**

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules, and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise, or defense of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

13. Information asset register/data inventory

13.1 BenevolentAI Group established a data inventory and data flow process in its DPA 2018 and UK GDPR / EU GDPR compliance programme. BenevolentAI Group's data inventory and data flow determine

- business processes that use personal data;
- source of personal data;
- the volume of data subjects;
- description of each item of personal data;
- processing activity;
- the process to maintain the inventory of data categories of personal data processed;
- how to document the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the BenevolentAI Group throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

13.2 BenevolentAI Group is aware of any risks associated with the processing of all particular types of personal data.

(a) BenevolentAI Group assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by BenevolentAI Group and in relation to processing undertaken by other organisations/processors on behalf of BenevolentAI Group.

(b) BenevolentAI Group shall manage any risks identified by the risk assessment in order to reduce the likelihood of non-conformance with this policy.

(c) Where a type of processing, in particular using new technologies and considering the nature, scope, context, and purposes of the processing is likely to result in a high-risk to the rights and freedoms of natural persons, BenevolentAI shall, prior to the processing, carry out a DPIA/PIA on the envisaged processing operations to ensure the protection of personal data. A single DPIA may address a set of similar processing operations that present similar levels of risks.

(d) Where, as a result of a DPIA it is clear that BenevolentAI Group is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not BenevolentAI Group may proceed will be escalated for review to the Data Protection Officer.

(e) The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress or the quantity of data concerned, escalate the matter to the supervisory authority.

(f) Appropriate controls will be selected as appropriate and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to BenevolentAI Group's documented risk acceptance criteria and the requirements of the UK GDPR and EU GDPR.

Document Owner

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements of the UK GDPR and the EU GDPR in line with BenevolentAI Group's objectives.

Versioning and Approval:

A current version (V1.8) of this document is available to all colleagues through the BenevolentAI Group's document management tool (MetaCompliance) with links provided on the Confluence page. Copies are held on the PIMS Programme repository on Google Drive. This procedure was reviewed by the General Counsel, and approved by the BenevolentAI Group's Chief Executive Officer (**CEO**).

It is issued on a version-controlled basis under his signature.

COMPLIANCE

Failure to comply with this procedure may impact the ability of the business to operate during times of crisis, as such, they may result in disciplinary action up to and including dismissal.

Approved by the Board on 17 September 2024.

Reference

INFO.EU: General Data Protection Regulation GDPR; https://gdpr-info.eu: (Accessed: 20/08/18)

ICO: Organisational Guide to the General Data Protection Regulation (GDPR); https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: 10/09/18)

CNPD: General Data Protection Regulation ; https://cnpd.public.lu/en/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees.html (Accessed: 24/03/22)

EDPB: GDPR: Guidelines, Recommendations, Best Practices; https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (Accessed: 14/09/18)

GOV.UK: Data Protection Act 2018; https://www.gov.uk/government/collections/data-protection-act-2018 (Accessed: 21/08/18)

LEGISLATION.OV.UK: The GDPR; http://www.legislation.gov.uk/ukpga/2018/12/part/2/chapter/2/enacted (Accessed: 15/09/18)