Data Protection and Privacy Policy

1. Introduction

Bellora Wealth Management ("the Company") is committed to ensuring the protection, privacy, and security of personal data in accordance with applicable data protection legislation, including the **UK General Data Protection Regulation (UK GDPR)**, the **EU General Data Protection Regulation (EU GDPR)**, the **Data Protection Act 2018**, and any other relevant data privacy laws.

This Data Protection and Privacy Policy ("the Policy") establishes the Company's approach to the collection, processing, storage, transfer, and deletion of personal data and affirms our commitment to lawful, fair, and transparent handling of personal information.

---

2. Purpose

The purpose of this Policy is to:

- Outline the principles and procedures for the protection of personal data;
- Define the responsibilities of the Company and its personnel in relation to data privacy;
- Ensure compliance with all applicable data protection laws;
- Safeguard the rights and freedoms of data subjects.

---

3. Scope

This Policy applies to:

- All employees, officers, directors, contractors, consultants, and temporary staff;
- All processing activities involving personal data carried out by the Company, whether in electronic, paper, or other formats;
- All systems, processes, and operations relating to personal data, irrespective of geographic location.

This Policy applies to both internal and external personal data, including that of clients, employees, partners, suppliers, and third parties.

---

4. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Data Subject:** The individual to whom the personal data relates.
- **Processing:** Any operation performed on personal data, whether automated or manual, such as collection, recording, storage, alteration, retrieval, use, disclosure, or erasure.
- **Controller:** The person or entity that determines the purposes and means of the processing of personal data.
- **Processor:** The person or entity that processes personal data on behalf of the controller.

---

5. Data Protection Principles

The Company adheres to the following principles of data protection as outlined in Article 5 of the UK/EU GDPR:

1. **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner.
2. **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimization:** Only data that is necessary for the intended purpose shall be collected and processed.
4. **Accuracy:** Data must be accurate and, where necessary, kept up to date.
5. **Storage Limitation:** Data must not be kept for longer than is necessary.
6. **Integrity and Confidentiality:** Data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss or damage.

7. **Accountability:** The Company is responsible for compliance with the above principles and must be able to demonstrate such compliance.

---

6. Lawful Basis for Processing

The Company will only process personal data where a lawful basis under Article 6 of the GDPR exists, including:

- The data subject has given **explicit consent**;
- Processing is necessary for the **performance of a contract**;
- Processing is required to comply with a **legal obligation**;
- Processing is necessary to protect the **vital interests** of the data subject;
- Processing is in the **legitimate interests** of the Company, provided those interests are not overridden by the rights of the data subject.

Where special categories of personal data are processed, the Company shall ensure compliance with Article 9 of the GDPR, including securing explicit consent or meeting another valid exemption.

---

7. Data Subject Rights

The Company recognises and upholds the following rights of data subjects:

- **Right to be informed** about the collection and use of their personal data;
- **Right of access** to their personal data;
- **Right to rectification** of inaccurate or incomplete data;
- **Right to erasure** (“right to be forgotten”);
- **Right to restrict processing** in certain circumstances;

- **Right to data portability**;
- **Right to object** to data processing;
- **Right not to be subject to automated decision-making** or profiling.

All requests from data subjects shall be handled in accordance with established procedures and responded to within the statutory timeframe of one month, unless extensions apply.

---

8. Data Security

The Company implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Access controls and authentication mechanisms;
- Encryption of sensitive data;
- Secure storage solutions;
- Data loss prevention systems;
- Regular risk assessments and audits;
- Confidentiality agreements for staff and third parties.

Employees are trained in data protection principles and required to report any actual or suspected data breaches without delay.

---

9. Data Breach Notification

In the event of a data breach, the Company shall assess the risk to data subjects and, if required, notify the **Information Commissioner's Office (ICO)** within **72 hours** of becoming aware of the breach. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, affected data subjects shall also be informed without undue delay.

---

10. International Data Transfers

Where personal data is transferred outside the UK or EEA, such transfers will only take place in accordance with Chapter V of the GDPR and will be subject to appropriate safeguards, such as:

- Adequacy decisions by the UK or European Commission;
- Standard Contractual Clauses (SCCs);
- Binding Corporate Rules (BCRs);
- Data Subject Consent, where appropriate.

---

11. Data Retention

Personal data shall be retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Data that is no longer required shall be securely destroyed or anonymized.

The Company maintains a **Data Retention Schedule** that specifies retention periods for various categories of data.

---

12. Third Party Processors and Contracts

Where third-party vendors process personal data on behalf of the Company, appropriate **Data Processing Agreements (DPAs)** shall be executed to ensure compliance with applicable data protection obligations.

The Company shall conduct due diligence prior to onboarding any third-party processor and shall monitor compliance throughout the business relationship.

---

13. Training and Awareness

The Company provides regular training and awareness programs to all staff to ensure a robust understanding of data protection responsibilities and obligations. Completion of data protection training is mandatory for all employees.

---

14. Governance and Accountability

The Board of Directors has overall responsibility for ensuring compliance with this Policy. Day-to-day operational responsibility lies with the appointed **Data Protection Officer (DPO)** or **Compliance Officer**, who shall oversee:

- Implementation of data protection measures;
- Response to data subject requests and breaches;
- Liaison with supervisory authorities;
- Maintenance of the **Record of Processing Activities (RoPA)**.

---

15. Policy Review

This Policy shall be reviewed annually and updated as necessary to reflect changes in legislation, regulatory guidance, or business practices.