INTEGER WEALTH GLOBAL

Policy Document

Data Protection

Issue: April 2024

1. Purpose

This Data Protection Policy outlines how Integer Wealth Global (IWG), a European-based financial services and investment management company registered in **Luxembourg, Liechtenstein, Gibraltar, and Cyprus**, collects, processes, stores, and protects personal data. The purpose is to ensure compliance with the **General Data Protection Regulation (EU) 2016/679 (GDPR)** and relevant national data protection laws.

2. Scope

This policy applies to:

- All personal data processed by IWG relating to clients, employees, contractors, partners, and third parties.
- All operations across IWG's offices in Luxembourg, Liechtenstein, Gibraltar, and Cyprus.
- All employees, consultants, and third-party service providers engaged in processing personal data on behalf of IWG.

3. Data Protection Principles

IWG adheres to the GDPR's core data protection principles:

- **Lawfulness, Fairness & Transparency** – Data is processed lawfully, fairly, and transparently.
- **Purpose Limitation** – Data is collected for specified, explicit, and legitimate purposes.
- **Data Minimisation** – Only the minimum necessary personal data is processed.
- **Accuracy** – Personal data is kept accurate and up to date.
- **Storage Limitation** – Data is retained only as long as necessary for legal and business purposes.
- **Integrity & Confidentiality** – Data is processed securely to prevent unauthorized access, loss, or damage.
- **Accountability** – IWG takes responsibility for demonstrating compliance with data protection laws.

4. Lawful Basis for Processing

IWG processes personal data based on one or more of the following lawful grounds:

- **Contractual necessity** – to deliver financial and investment services.
- **Legal obligation** – to comply with EU and national financial regulations, anti-money laundering (AML) laws, and tax reporting obligations.
- **Legitimate interests** – to manage business operations, improve services, and ensure security.
- **Consent** – for specific processing activities, such as marketing communications.

5. Data Subjects' Rights

In accordance with GDPR, data subjects have the following rights:

- Right to access their personal data.
- Right to rectification of inaccurate data.
- Right to erasure ("right to be forgotten") where legally permissible.
- Right to restrict or object to processing.
- Right to data portability.
- Right to withdraw consent (where processing is based on consent).
- Right to lodge a complaint with the relevant Data Protection Authority.

6. Data Security Measures

IWG implements appropriate technical and organizational measures to ensure a high level of data protection, including:

- Encryption of digital records.
- Secure storage and controlled access to sensitive data.
- Multi-factor authentication for internal systems.
- Regular penetration testing and security audits.
- Physical safeguards for office premises and archived records.
- Employee training on data protection responsibilities.

7. Data Sharing and Transfers

- Personal data may be shared with regulators, auditors, and legal authorities as required by law.
- Third-party service providers are bound by data processing agreements to ensure GDPR compliance.
- Where personal data is transferred outside the European Economic Area (EEA), IWG ensures adequate safeguards (e.g., Standard Contractual Clauses).

8. Data Retention

- Client records: retained for at least **7 years** in compliance with financial regulations.
- Employee records: retained for the duration of employment and up to **6 years** post-termination.
- Marketing data: retained until consent is withdrawn.
  A detailed retention schedule is maintained and reviewed regularly.

9. Roles and Responsibilities

- **Board of Directors**: Provides oversight and ensures compliance with applicable regulations.
- **Data Protection Officer (DPO)**: Responsible for monitoring compliance, advising on obligations, and serving as point of contact with supervisory authorities.
- **Employees and Contractors**: Must adhere to this policy and undergo regular data protection training.

10. Breach Notification

- All data breaches must be reported immediately to the DPO.
- IWG will notify the relevant supervisory authority within **72 hours** of becoming aware of a breach, where required by GDPR.
- Affected data subjects will be informed without undue delay if the breach is likely to result in high risk to their rights and freedoms.

11. Policy Review

This policy will be reviewed **annually**, or earlier if required by changes in regulation, business operations, or supervisory authority guidance.