HEAD OFFICE
Room 2201, 22/F
28 Stanley Street • Central • Hong Kong
Tel: + 852 2168 0686

Global Investment Strategy HK Ltd

GDPR DATA PROTECTION POLICY

GLOBAL INVESTMENT STRATEGY HONG KONG

HEAD OFFICE
Room 2201, 22/F
28 Stanley Street • Central • Hong Kong
Tel: + 852 2168 0686

Contents

GLOBAL INVESTMENT STRATEGY HONG KONG

HEAD OFFICE
Room 2201, 22/F
28 Stanley Street • Central • Hong Kong
Tel: + 852 2168 0686

Personal Data (Privacy) Ordinance (Cap. 486) – Data Protection Policy (Hong Kong)

Entity: Global Investment Strategy HK Limited
Jurisdiction: Hong Kong SAR
Last updated: 05 May 2026
Version: 1.1 – Hong Kong PDPO & SFC aligned

1. Purpose and Scope
This Policy sets out how Global Investment Strategy HK Limited (the "Firm") manages personal data in compliance with the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") and in line with expectations of the Securities and Futures Commission ("SFC") regarding governance, internal controls and data protection. The Policy applies to all personal data collected, held, processed or transmitted by the Firm in or from Hong Kong.

2. Regulatory Framework
This Policy is informed by the six Data Protection Principles (DPPs) under Schedule 1 of the PDPO, guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD), and SFC expectations under the Code of Conduct and the Management, Supervision and Internal Control Guidelines for Licensed Corporations.

3. Governance and Accountability
The Board and Senior Management retain overall responsibility for data protection and cyber resilience. Senior Management ensures that adequate resources, controls and oversight arrangements are in place to manage personal data risks, consistent with SFC expectations on accountability and effective management oversight.

4. Data Protection Principles
- DPP1 – Purpose and Manner of Collection: Personal data is collected lawfully, fairly, and for purposes directly related to the Firm's regulated activities.
- DPP2 – Accuracy and Retention: Personal data is kept accurate and is not retained longer than necessary, taking account of regulatory record-keeping obligations.
- DPP3 – Use of Personal Data: Personal data is used only for its stated purpose or a directly related purpose, unless prescribed consent has been obtained.
- DPP4 – Security: The Firm applies proportionate technical and organisational measures, including access controls and system security, to safeguard personal data.
- DPP5 – Openness: Information on the Firm's data protection policies and practices is made available in a transparent manner.
- DPP6 – Access and Correction: Data subjects may request access to and correction of personal data in accordance with statutory requirements.

HEAD OFFICE
Room 2201, 22/F
28 Stanley Street • Central • Hong Kong
Tel: + 852 2168 0686

5. Data Subject Rights
Individuals may submit written requests for access to or correction of their personal data. Requests are assessed and responded to within the statutory timeframe (generally 40 days), subject to applicable exemptions under the PDPO.

6. Use, Transfer and Outsourcing
Personal data may be transferred to third-party service providers or group entities where necessary. In line with SFC expectations on outsourcing and use of external service providers, appropriate due diligence, confidentiality obligations and contractual safeguards are applied.

7. Data Security and Cyber Resilience
The Firm maintains information security arrangements proportionate to its business and risk profile. Controls include access management, system security, staff awareness and incident monitoring, consistent with SFC expectations regarding the protection of client and confidential information.

8. Data Incident Management
All suspected data incidents are escalated promptly to Compliance and Senior Management. While PDPO breach notification is not mandatory, the Firm follows PCPD and SFC good practice by assessing materiality and notifying regulators or affected individuals where appropriate.

9. Training and Awareness
Staff receive periodic training on data protection, confidentiality and information security. Training is tailored to roles and responsibilities, supporting SFC expectations for staff competence and awareness of regulatory obligations.

10. Review and Monitoring
Compliance monitors adherence to this Policy and reports material issues to Senior Management. The Policy is reviewed periodically to ensure continued compliance with PDPO requirements and evolving SFC expectations.