1. INTRODUCTION

Business Class Group ("the Group"), incorporating all the operating brands in Hong Kong and all jurisdictions in which BCG has a presence, is committed to safeguarding the privacy, confidentiality, and security of personal data. This Policy explains how personal information is collected, used, processed, stored, transferred, and protected across the Group's operations in Hong Kong, the United Kingdom, China and any other jurisdictions in which the Group conducts business.

The Group complies with the strictest applicable legislation, including:

- Personal Data (Privacy) Ordinance (PDPO) – Hong Kong
- UK GDPR (General Data Protection Regulation)
- PIPL (Personal Information Protection Law) – China

This Policy applies to all individuals acting on behalf of the Group and to all personal data processed by the Group. All Group companies and brands who are directly authorised or regulated will follow the rules and guidelines of their lead regulator, any companies not directly authorised will apply Hong Kong Insurance Authority regulatory standards as the minimum requirement.

2. SCOPE

This Policy applies to:

- Employees
- Consultants and appointed representatives
- Contractors
- Third-party service providers
- Any individual handling personal data on behalf of the Group

It covers all data processed through:

- Client onboarding
- HR & employment
- Marketing (consent-based)
- Digital platforms and communication systems
- Third-party vendor arrangements

3. DEFINITIONS

Personal Data
Any information relating to an identified or identifiable individual.

Special Category/Sensitive Data
Includes (but is not limited to) biometric data, ethnicity, religious beliefs, health data, financial account data, government identifiers, and minors' data.

Processing
Any operation performed on personal data, including collection, storage, transfer, use, analysis, or deletion.

Data Subject
The individual to whom the data relates.

4. DATA PROTECTION PRINCIPLES

The Group follows internationally recognised principles:

4.1. Lawfulness, Fairness & Transparency

Data must be processed lawfully and transparently.

4.2. Purpose Limitation

Data must be used only for legitimate and disclosed purposes.

4.3. Data Minimisation

Collect only what is necessary.

4.4. Accuracy

Keep data accurate and up to date.

4.5. Storage Limitation

Do not retain data longer than required.

4.6. Integrity & Confidentiality

Protect data using appropriate technical and organisational controls.

4.7. Accountability

The Group must demonstrate compliance with all relevant regulations.

5. COLLECTION OF PERSONAL DATA

Personal data may be collected for:

- Client onboarding and KYC/CDD
- AML/CTF screening
- Suitability assessments
- HR and employment administration
- Marketing (with consent)
- Regulatory obligations
- Policy and investment administration
- System monitoring and security

Data may be collected through online forms, onboarding documentation, emails, calls, digital tools, or direct interaction.

6. USE OF PERSONAL DATA

Personal data may be used for:

- Providing consulting, advisory, insurance, property and investment services
- Performing due diligence and compliance & AML checks
- Fulfilling contractual and regulatory obligations
- Internal analytics and reporting
- HR administration
- Marketing communications (only with valid consent)
- Fraud detection and prevention
- IT security and system monitoring

Data will not be used for purposes inconsistent with those disclosed.

7. DISCLOSURE OF PERSONAL DATA

Data may be shared with:

- Insurers, product and service providers
- Banks, custodians, and financial institutions
- Regulators (IA, TCSP, EAA, FCA, OIC, PBOC, etc.)
- External legal and professional advisers
- IT service providers and vendors
- Third-party processors with contractual safeguards

All third parties must comply with Group privacy standards.

8. CROSS-BORDER DATA TRANSFERS

Transfers may occur between Group companies or to third parties overseas, but only when:

- Required for service delivery
- Appropriate safeguards are in place
- Transfers comply with PDPO, GDPR, PIPL

GDPR requirements

Adequacy decisions, Standard Contractual Clauses (SCCs), or equivalent safeguards.

PIPL requirements

Security assessments, standard contracts, or certification mechanisms.

PDPO

Best-practice contractual safeguards recommended.

9. DATA SUBJECT RIGHTS

Data subjects may exercise rights including:

Hong Kong (PDPO)

- Access
- Correction

UK/EU (GDPR)

- Access, rectification, deletion
- Restrict processing
- Data portability
- Object to processing
- Rights relating to automated decisions

China (PIPL)

- Access, correction, deletion
- Restrict automated processing
- Explanation of processing rules

The Group will respond to requests within statutory timelines.

10. DATA RETENTION

Data will be retained for at least:

- 7 years (general regulatory requirements)
- 5–7 years for AML/CTF data
- 7 years for HR/employment files
- Duration of the client relationship + 7 years

Data must be securely stored, encrypted where required, and restricted to authorised personnel.

11. SECURITY MEASURES

Security protocols include:

- Encryption and secure storage
- Multi-factor authentication
- Password protection
- Access control & role-based restrictions
- Network segmentation
- IT monitoring and cybersecurity systems
- Staff training
- Vendor security assessments

Any suspected breach must be reported immediately to Compliance and IT.

12. ARTIFICIAL INTELLIGENCE (AI) & PRIVACY

AI may be used to support:

- Document structuring
- AML/CTF screening support
- Pattern identification
- Internal analysis

AI must not:

- Process confidential or personal data using unapproved tools
- Make suitability, compliance, or onboarding decisions
- Conduct automated profiling without human review
- Circumvent privacy or security controls

AI must comply with:

- Hong Kong OGCIO Ethical AI principles
- GDPR automated decision rules
- China PIPL algorithmic transparency requirements
- Global Fairness Standards

13. THIRD-PARTY PROCESSORS

Third parties handling personal data must:

- Undergo due-diligence checks
- Sign Data Processing Agreements (DPAs)
- Maintain adequate cybersecurity controls
- Permit audits or reviews
- Process data only as instructed

Vendors failing to comply may be terminated.

14. DIRECT MARKETING

Direct marketing may only be conducted when:

- Explicit consent has been obtained
- The purpose is clearly explained
- Opt-out options are provided
- Records of consent are kept
- Withdrawals of consent are honoured promptly

Marketing must comply with PDPO/GDPR/PIPL.

15. DATA BREACH MANAGEMENT

In the event of a data breach:

1. Contain the breach
2. Assess the impact
3. Notify Compliance immediately
4. Determine regulatory notification requirements
   - GDPR: 72-hour rule
   - PIPL: high-risk breaches require notification
5. Notify affected individuals where harm is likely
6. Document the incident
7. Implement remediation

16. RESPONSIBILITIES

All Staff

- Protect data
- Follow policies
- Report incidents

Managers

- Oversee compliance
- Support staff training
- Implement corrective actions

Compliance

- Monitoring and oversight
- Supporting data subject requests
- Advising on regulatory requirements

IT

- Maintaining security controls
- Managing breaches and system incidents

Senior Management

- Governance and oversight
- Ensuring adequate resources

17. REVIEW OF POLICY

This Policy will be reviewed annually or earlier if:

- Regulatory changes occur
- Business processes change
- New technologies introduce privacy risks

APPENDIX— DATA SUBJECT RIGHTS, LAWFUL BASIS & TRANSFER CHECKLIST

1. Data Subject Rights Matrix

Jurisdiction	Access	Delete	Portability	Automated Decision Rights
PDPO (HK)	✓	Limited	✓	Limited
GDPR (UK/EU)	✓	✓	✓	✓
PIPL (China)	✓	✓	✓	✓

2. Lawful Bases for Processing

- Contractual Necessity – providing services, onboarding, administration
- Legal Obligation – AML/CTF, regulatory reporting
- Consent – marketing, optional services
- Legitimate Interests – internal operations, fraud prevention
- Vital Interests – safety and emergency situations

3. Cross-Border Transfer Checklist

Before transferring personal data overseas:

- Confirm legal basis
- Use appropriate safeguards (SCCs/PIPL Contract requirements)
- Verify vendor compliance
- Update Record of Processing Activities
- Notify the data subject where required

Data Breach Severity Levels

Level	Description	Notification Required
Low	No meaningful risk	No
Medium	Potential harm	Case-by-case
High	Likely harm	Regulator + Data Subjects
Critical	Serious risk, sensitive data, widespread breach	Mandatory Notifications