PRIVACY POLICY

Contents

1. Introduction

DPRG IM Ltd with Registration Number: HE433850, (hereinafter referred to as the "Company") is committed to protecting the privacy and personal data of all individuals with whom it engages in the course of providing investment services. This Privacy Policy outlines the Company's approach to the collection, processing, use, storage, and protection of personal data, in compliance with applicable data protection laws and regulatory obligations.

The Policy applies to all personal data received or generated by the Company in the context of its operations as a Cyprus Investment Firm (CIF), licensed and regulated by the Cyprus Securities and Exchange Commission (CySEC) with license number 454/25. The Company is dedicated to processing personal data transparently, lawfully, fairly, and securely, ensuring that all individuals' rights are safeguarded at all times.

This Policy has been drafted and is maintained in accordance with the following applicable legal and regulatory framework:

- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)
- Cyprus Law 125(I)/2018, which implements the GDPR nationally
- Law 87(I)/2017 regarding the provision of investment services and related matters (MiFID II Law)
- Law 188(I)/2007 on the Prevention and Suppression of Money Laundering and Terrorist Financing (AML Law)
- Directive (EU) 2015/849 (4th AML Directive)
- Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)
- CySEC Directive DI87-01 regarding product governance and safeguarding of client assets
- CySEC Circulars C031, C138, and C030 on remuneration, compliance, and governance
- Any other applicable circulars, regulatory guidelines, or implementing provisions issued by CySEC, the Office of the Commissioner for Personal Data Protection, or the European Data Protection Board (EDPB)

This Privacy Policy is designed to ensure that:

- Individuals understand how and why their personal data is processed by the Company;
- The Company complies with all legal and regulatory requirements concerning data protection;
- Appropriate safeguards and governance measures are in place to manage personal data risks;
- All relevant stakeholders, including clients, partners, and staff, are informed of their rights and the Company's obligations.

Further sections of this Policy explain the specific types of personal data processed, the legal basis for processing, data subject rights, security measures, and the Company's approach to compliance, breach management, and digital operational resilience in line with DORA.

2. Scope and Application

This Privacy Policy applies to all personal data processed by the Company in its capacity as a data controller, in accordance with Article 4(7) of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). It covers the data of natural persons who interact with the Company in any capacity, whether as clients, employees, job applicants, contractors, business partners, website users, or other third parties.

The Policy applies to all departments, business units, and service lines of the Company and governs all forms of processing, whether performed manually or through automated means, including but not limited to collection, recording, organisation, storage, alteration, retrieval, use, disclosure, transmission, combination, erasure, or destruction of personal data.

Specifically, this Policy applies to the following categories of data subjects:

- Clients: Individuals who have entered into or are considering entering into an investment services relationship with the Company
- Employees and Job Applicants: Individuals currently employed by the Company, or those applying for employment

- Contractors and Service Providers: Natural persons engaged directly or via third-party arrangements who perform work or services for the Company

- Directors and Shareholders: Board members, UBOs, or significant shareholders whose information is collected as part of regulatory or due diligence obligations

- Website Visitors: Individuals who visit, browse, or interact with the Company's website or digital platforms

- Any Other Individuals: Including complainants, correspondents, regulatory contacts, or individuals identified through KYC, AML, or compliance procedures

This Policy also applies to:

- All personal data processed in the context of the Company's activities, regardless of where the data is stored or accessed (e.g., cloud, on-premises, offsite storage)

- All employees and external parties who process personal data on behalf of the Company, including outsourced service providers, IT support staff, and legal or compliance advisors.

In addition, this Policy operates in conjunction with the Company's internal frameworks on digital operational resilience and ICT risk management, in alignment with Regulation (EU) 2022/2554 (DORA). Personal data processing that relies on or is exposed to digital infrastructure is governed by DORA's principles for ICT security, business continuity, and third-party risk management, and falls within the scope of this Policy.

This Policy does not apply to anonymised data or information that does not relate to an identified or identifiable individual, provided it has been processed in a manner that prevents re-identification.

The Company expects all employees and contractors to familiarise themselves with this Policy and adhere to its principles. Non-compliance may result in disciplinary measures, contractual penalties, or legal consequences, depending on the severity of the breach.

3. Definitions

For the purposes of this Privacy Policy, the following definitions shall apply, as derived from the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Cyprus Data Protection Law, Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA),

and other applicable European and national data protection legislation. These terms form the foundation for understanding the Company's approach to privacy, cybersecurity, and data protection:

- Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier (e.g., IP address), or 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 that is inherently more sensitive and requires enhanced protection. This includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, health-related data, or data concerning a person's sex life or sexual orientation.

- Processing: Any operation or set of operations performed on personal data, whether or not by automated means. This includes, but is not limited to, 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.

- Data Subject: Any identified or identifiable natural person whose personal data is collected, held, or otherwise processed by the Company. Data subjects may include, but are not limited to, clients, employees, contractors, website users, or any individual interacting with the Company in the context of its business activities.

- Data Controller: The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, The Company acts as the Data Controller for all personal data it collects and processes in the course of its activities.

- Data Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller, according to instructions received. Processors may include external service providers such as IT support firms, payroll providers, or cloud hosting companies.

- Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, through a statement or clear affirmative action, signify

agreement to the processing of personal data relating to them.

- Supervisory Authority: The independent public authority responsible for overseeing and enforcing the application of data protection law. In Cyprus, this is the Office of the Commissioner for Personal Data Protection.

- Data Breach: A security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Company or its processors. Data breaches may occur as a result of cyberattacks, internal errors, or negligent handling of data.

- Anonymisation: The process by which personal data is irreversibly altered in such a way that the data subject can no longer be identified, either directly or indirectly. Properly anonymised data falls outside the scope of data protection legislation.

- Pseudonymisation: The processing of personal data in such a way that it 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 subject to technical and organisational measures to ensure non-attribution.

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

- Digital Operational Resilience: As defined under DORA, this refers to the ability of financial entities to build, assure, and review their operational integrity and security against ICT-related disruptions, threats, and failures.

- ICT Third-Party Provider: Under DORA, any external provider that supplies digital services, platforms, or systems that could affect the operational resilience of the Company and its handling of personal data.

These definitions are used consistently throughout this Policy to ensure clarity and alignment with applicable laws and regulatory expectations, including GDPR and DORA.

4. Data Subjects Covered by this Policy

This Privacy Policy applies to all natural persons whose personal data is collected, held, or otherwise processed by the Company in the context of its business operations, regulatory

obligations, and contractual relationships. This includes any individual who interacts with the Company in the capacity of client, employee, contractor, online user, visitor, partner, regulator, or third party whose data is captured in the course of compliance, AML, or risk-related procedures. The individuals whose data may be processed under this Policy ("data subjects") fall into the following main categories:

4.1 Clients and Prospective Clients

Natural persons who receive or express an interest in receiving investment services, ancillary services, or any other offerings provided by the Company. This includes both retail and professional clients, as well as eligible counterparties, as defined under MiFID II. The personal data of such individuals is processed for the purposes of onboarding, client due diligence (CDD), suitability assessments, contractual execution, and ongoing service provision.

4.2 Employees, Job Applicants, and Interns

This includes:

- Individuals who are currently employed or engaged by the Company under any form of employment contract (e.g., permanent, temporary, part-time, or fixed-term);
- Individuals who apply for a role at the Company or are shortlisted during recruitment processes;
- Trainees, interns, or seconded personnel.

The processing of their data covers recruitment, payroll, human resource management, performance monitoring, training, health and safety, and compliance with employment law.

4.3 Contractors and External Service Providers

Natural persons who provide outsourced or consulting services directly to the Company, either in an individual capacity or through third-party entities. These may include IT consultants, legal and audit professionals, marketing service providers, and independent compliance advisors. The processing of their personal data typically relates to contractual performance, compliance verifications, and due diligence assessments.

4.4 Company Directors, Officers, and Shareholders

This includes the members of the Board of Directors, executive officers, and individuals who hold ownership or control interests in the Company. Their data is processed in accordance with regulatory obligations under the AML Law, MiFID II, and the Company's internal governance

policies (e.g., for conflict-of-interest registers, fitness and probity assessments, and disclosures to CySEC).

4.5 Visitors to the Company's Premises or Website

- Visitors to premises: Natural persons whose personal data is collected in the context of physical security and visitor log management (e.g., name, ID, time of entry).

- Website users: Natural persons who browse or interact with the Company's websites or online portals. Information processed may include IP addresses, cookies, and data entered into forms, as governed by the Company's Cookie and Website Privacy Notices.

4.6 Business Partners, Vendors, and Other Counterparties

Individuals who represent or are associated with legal entities or organisations that the Company collaborates with in a commercial or professional context. Their data is processed for contract management, regulatory reporting, AML screening, and communications.

4.7 Regulatory and Supervisory Authorities

Natural persons acting on behalf of public institutions, such as CySEC or the Office of the Commissioner for Personal Data Protection. Personal data may be processed during official correspondence, inspections, or reporting obligations.

4.8 Complainants, Enquirers, and Other Correspondents

Natural persons who contact the Company to submit a complaint, raise an enquiry, or otherwise correspond with the Company in any capacity, whether on their own behalf or on behalf of others.

4.9 Other Individuals Identified via Compliance, AML or Risk Procedures

This may include individuals who are referenced during:

- Know Your Customer (KYC) checks

- Politically Exposed Persons (PEP) assessments

- Adverse media screening

- Suspicious transaction investigations

- Conflict of interest reviews or whistleblowing mechanisms
- Digital Operational Resilience testing or incident detection under Regulation (EU) 2022/2554 (“DORA”), where natural persons are involved in ICT-related events or have been indirectly affected by operational incidents.

This Policy is intended to ensure transparency and consistency in how the Company processes personal data across all relevant categories of data subjects, whether the interaction is direct or indirect, online or offline, or regulated by GDPR, national law, or DORA.

5. Categories of Personal Data Collected

In the course of its operations, the Company collects and processes various categories of personal data for purposes directly related to the provision of investment services, the fulfilment of legal obligations, and the proper administration of internal operations.

The nature and extent of the data collected depends on the data subject’s relationship with the Company, applicable regulatory requirements, and the specific processing purpose. The categories of personal data processed by the Company include, but are not limited to, the following:

5.1 Identification and Contact Information

These data are collected to establish the identity of individuals and maintain communication:

- Full name
- Residential and/or correspondence address
- Email address(es)
- Landline and mobile phone number(s)
- Date and place of birth
- Gender
- Nationality and citizenship

5.2 Verification and Legal Documentation

Collected for KYC, CDD, AML, and regulatory onboarding processes:

- National ID card or passport details (including document number, expiry date, issuing country)
- Utility bills or bank statements for address verification
- Tax Identification Number (TIN)
- Social insurance or national registration numbers
- Marital status and family details (where legally required)

As part of its regulatory obligations under AML and counter-terrorism financing (CTF) laws, the Company also conducts screening of all clients and related parties against international sanctions lists, watchlists, and politically exposed persons (PEPs) databases. This includes screening against UN, EU, OFAC, and other applicable sanctions regimes. The information processed typically includes full name, nationality, date of birth, and identification number.

5.3 Financial and Economic Data

Required for client profiling, suitability assessments, onboarding, and regulatory reporting:

- Bank account numbers and IBANs
- Source of funds and source of wealth information
- Annual income and estimated net worth
- Employment and occupation details
- Financial objectives, risk tolerance, and investment experience
- Credit or solvency information (if applicable)

5.4 Transactional and Account Data

Collected through the provision of services and related operations:

- Trading activity and order history
- Asset holdings and portfolio positions
- Transaction values, dates, and payment methods
- Internal account numbers and client classification status

5.5 Employment and HR-Related Data

Applicable to employees, interns, and job applicants:

- Curriculum vitae (CV), education history, and professional qualifications
- Employment contracts and payroll data
- Attendance, leave, and time tracking records
- Disciplinary or grievance records
- Evaluation and performance review records
- Work permits and right-to-work documentation

5.6 Website, IT, and System Usage Data

Collected automatically or via Company systems, critical under DORA for ensuring ICT-related risk monitoring and digital operational resilience:

- IP addresses, device/browser data
- Login credentials and usage logs
- Access to internal platforms
- Geolocation or access history
- Activity tracking within digital environments (e.g., CRM, trading portal)

- System logs, intrusion alerts, audit trails, and error reports, which are processed for security monitoring, as required under DORA

- Technical identifiers related to ICT third-party services (e.g., cloud login metadata, system health checks)

5.7 Special Categories of Personal Data (Sensitive Data)

In rare and limited cases, the Company may collect special categories of personal data where required by law or with explicit consent, including:

- Health information (e.g., medical certificates for employee leave or COVID-19 reporting)

- Biometric identifiers (e.g., security or access control systems)

- Criminal record declarations or background checks (where legally required)

- Information revealing political opinions or affiliations (only if disclosed incidentally during due diligence or onboarding)

Note: Political exposure status (i.e., whether an individual qualifies as a Politically Exposed Person, or "PEP") and sanctions screening are performed for all clients under AML legislation. This data is not treated as special category under GDPR unless it reveals protected characteristics, such as political opinions.

The Company ensures that such data is processed only when strictly necessary, in accordance with Article 9 of the GDPR, and with enhanced safeguards and restricted access.

5.8 Communication Records and Correspondence

- Emails, letters, chat transcripts, and telephone call recordings with clients or staff

- Complaints, feedback forms, or regulatory correspondence

- Internal memos and reporting documentation

5.9 Marketing and Consent Preferences

- Opt-in/opt-out preferences

- Consent records (e.g. cookie banners, email campaigns)

In line with DORA, the Company ensures that personal data collected through ICT systems is subject to security measures, real-time monitoring, and logging to support digital operational resilience, particularly for detecting and mitigating ICT-related incidents.

All personal data is processed in accordance with the principle of data minimisation, meaning only data that is necessary for the relevant processing purpose is collected and retained

6. Purposes and Legal Bases for Processing

The Company collects and processes personal data only to the extent necessary for lawful, specific, and legitimate purposes. All processing is performed in accordance with the principles of fairness, transparency, and accountability as outlined in Article 5 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), and applicable national laws, including the Investment Services Law 87(I)/2017, the Prevention and Suppression of Money Laundering Law 188(I)/2007, and the DORA Regulation (EU) 2022/2554 on digital operational resilience in the financial sector.

The main purposes for which the Company processes personal data, along with the corresponding legal bases, are outlined below:

6.1 Client Onboarding and Know Your Customer (KYC) Procedures

Purpose: Verifying the identity of clients, conducting due diligence checks, and assessing risk profiles in compliance with AML obligations.

Legal Basis:

- Article 6(1)(c) GDPR – Compliance with a legal obligation (e.g., AML Law, MiFID II)
- Article 6(1)(e) GDPR – Processing in the public interest (e.g., financial crime prevention)

6.2 Provision of Investment Services

Purpose: Delivering the services agreed under the client agreement, including portfolio management, execution of orders, and account maintenance.

Legal Basis:

- Article 6(1)(b) GDPR – Necessary for the performance of a contract
- Article 6(1)(c) GDPR – Compliance with MiFID II and related regulatory obligations

6.3 Regulatory and Legal Compliance

Purpose: Fulfilling the Company's obligations under CySEC rules, MiFID II, AML directives, DORA, tax reporting laws, and audit requirements.

Legal Basis:

- Article 6(1)(c) GDPR – Compliance with a legal obligation

6.4 Employment and Human Resources Administration

Purpose: Managing employee contracts, payroll, benefits, leave, performance reviews, and compliance with employment law.

Legal Basis:

- Article 6(1)(b) GDPR – Necessary for the performance of a contract
- Article 6(1)(c) GDPR – Compliance with employment and tax laws
- Article 6(1)(f) GDPR – Legitimate interests (e.g., maintaining internal operations)

6.5 Risk Management and Internal Controls

Purpose: Monitoring systems and behaviour to detect fraud, insider trading, market abuse, or ICT-related risks, and to uphold compliance with internal policies and procedures.

Legal Basis:

- Article 6(1)(c) GDPR – Compliance with legal obligations
- Article 6(1)(f) GDPR – Legitimate interests (e.g., safeguarding the integrity of services)

  Note (DORA Integration): Pursuant to DORA, this includes monitoring of information and communication technology (ICT) systems, logging of access and activity, and implementing operational resilience measures to protect personal data against ICT

disruptions.

6.6 Communication and Customer Support

Purpose: Responding to enquiries, providing information, and supporting clients via various communication channels.

Legal Basis:

- Article 6(1)(b) GDPR – Necessary for the performance of a contract
- Article 6(1)(f) GDPR – Legitimate interests (e.g., ensuring customer satisfaction)

6.7 Marketing and Promotions

Purpose: Sending newsletters, event invitations, or promotional material (subject to consent or soft opt-in, where applicable).

Legal Basis:

- Article 6(1)(a) GDPR – Consent (for direct marketing)
- Article 6(1)(f) GDPR – Legitimate interests (e.g., marketing to existing clients)

Note: Individuals can withdraw consent or opt out of marketing communications at any time.

6.8 Website Operation and Security Monitoring

Purpose: Enabling the proper functioning, security, and performance of the Company's website and IT systems, including usage analytics, access control, and incident detection.

Legal Basis:

- Article 6(1)(f) GDPR – Legitimate interests (e.g., system integrity, analytics)

  Note (DORA Integration): Under DORA, such processing includes real-time ICT security monitoring, detection of anomalous behaviour, and reporting of ICT-related incidents that may affect personal data integrity or availability.

6.9 Legal Claims and Dispute Resolution

Purpose: Establishing, exercising, or defending legal claims in judicial or administrative proceedings.

Legal Basis:

- Article 6(1)(f) GDPR – Legitimate interests
- Article 9(2)(f) GDPR – Where special categories of data are involved (e.g., health data in an employment dispute)

6.10 Processing of Special Categories of Data

In certain limited cases, the Company may process sensitive personal data, such as health data for sick leave or biometric data for secure access control.

Legal Basis:

- Article 9(2)(a) GDPR – Explicit consent
- Article 9(2)(b) GDPR – Employment law obligations
- Article 9(2)(g) GDPR – Substantial public interest (e.g., AML screening)

7. Data Collection Methods and Sources

The Company collects personal data from a variety of sources, depending on the nature of the relationship with the data subject and the specific services or obligations involved. Data is collected either directly from the individual or, where appropriate, from third-party or publicly available sources, in full compliance with the principles of lawfulness, fairness, and transparency as set out in Article 5 of the GDPR. In line with Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), the Company ensures that data collected through ICT systems is logged, monitored, and subject to security controls to prevent unauthorised access or alteration.

7.1 Data Collected Directly from the Data Subject

The majority of personal data processed by the Company is obtained directly from the data subject, typically at the time of: account registration or onboarding procedures; submission of application forms or other client documentation; completion of employment-related documentation (e.g. job applications, contracts); participation in due diligence or KYC processes; communication with the Company (e.g. email, phone calls, in-person meetings);

access or interaction with the Company's website, platforms, or digital services; engagement in events, training sessions, or other Company-hosted activities. During such interactions, individuals may be asked to provide identifying information (e.g. name, address, ID), financial information, employment history, educational background, or any other data required for the purpose of compliance, service provision, or communication.

7.2 Data Collected from Third Parties

In accordance with GDPR Article 14, the Company may also obtain personal data from third-party sources where legally permissible. These sources include: credit reference agencies and risk intelligence providers; publicly accessible databases or registers (e.g., company registries, land records); regulatory authorities or law enforcement bodies (e.g., in the context of AML/CFT obligations); external consultants or service providers involved in onboarding or compliance support; business partners or intermediaries introducing clients to the Company; former employers or references (in the context of recruitment). When data is collected from third parties, the Company informs the data subject of the processing in accordance with its obligations under Articles 14(3)–(5) of the GDPR, unless an exemption applies.

7.3 Data Collected Automatically

The Company also collects certain categories of personal data automatically when individuals interact with its website or digital systems. This includes: IP addresses, device identifiers, and browser types; website usage statistics and access logs; cookies and similar technologies used for user authentication, website optimisation, or security. Such data is used to improve user experience, secure the digital environment, and monitor system performance. Where required, the Company obtains user consent for the deployment of non-essential cookies in accordance with applicable ePrivacy regulations. In line with DORA, such ICT-derived data is securely logged and monitored to enhance operational resilience, including detection and prevention of ICT-related incidents and disruptions.

7.4 Data Accuracy and Minimisation

The Company takes reasonable steps to ensure that all personal data collected is accurate and up to date, relevant and limited to what is necessary for the intended purpose (data minimisation), and obtained through lawful and transparent means. Where applicable, data subjects are encouraged to inform the Company of any changes to their personal information to help maintain accuracy and integrity.

8. Data Retention and Storage

The Company adopts a structured and risk-based data retention framework that ensures personal data is stored only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable legal, regulatory, or contractual obligations. The Company's data

retention practices are governed by the principles of storage limitation, accountability, and confidentiality, as outlined in Article 5(1)(e) and Article 32 of the General Data Protection Regulation (GDPR), and aligned with the Digital Operational Resilience Act (DORA) requirements for data and ICT risk management.

8.1 General Retention Principles

The Company retains personal data:

• For the duration of the contractual or service relationship with the data subject

• As long as is necessary to comply with statutory or regulatory obligations

• Until the expiry of legal limitation periods for claims or disputes

• Until consent is withdrawn (where processing is based on consent), subject to any overriding legal grounds for continued processing

Retention periods are reviewed regularly for necessity and proportionality. The Company ensures that retention rules are aligned with operational resilience obligations under DORA, including continuity of critical operations and secure data management.

8.2 Regulatory and Legal Retention Requirements

Certain categories of personal data are retained in accordance with specific legal and regulatory obligations, including but not limited to:

• Investment services data: Retained for a minimum of five (5) years from the end of the client relationship under Law 87(I)/2017 and CySEC Directive DI87-01, and up to seven (7) years if required by CySEC

• AML-related records: Retained for five (5) years from the date of transaction or relationship termination, in accordance with AML Law 188(I)/2007

• Employment data: Retained for the period of employment and up to six (6) years thereafter, as per labour and tax laws

• Website logs and digital tracking data: Retained for 12 to 24 months, depending on system configuration and purpose

• ICT log and monitoring data: Retained in accordance with DORA Article 9, which requires secure storage of ICT-related logs to support incident detection, investigation, and reporting

8.3 Secure Storage of Personal Data

The Company stores personal data in secure electronic and physical environments with access limited to authorised personnel. Storage systems include:

• On-premise servers and encrypted drives for internal operations

• Cloud-based solutions hosted within the EEA or subject to appropriate safeguards

• Document management systems with user access controls and audit trails

The Company ensures that security controls around storage locations meet the resilience and traceability requirements of DORA, particularly for ICT-related services and backups.

8.4 Archiving, Disposal, and Anonymisation

When the retention period expires and no further legal basis for storage exists, the Company proceeds with one of the following:

• Secure deletion using data erasure tools or shredding for paper documents

• Anonymisation for statistical, compliance, or audit purposes, where data re-identification is no longer required

• Restricted archival for legal, regulatory, or continuity reasons

Disposal logs are maintained and monitored in accordance with the Company's Information Security Policy and DORA's requirements for ICT continuity and incident traceability.

8.5 Responsibility and Oversight

The Data Protection Officer (DPO), in coordination with the Information Security and Compliance Departments, oversees the Company's retention practices. Responsibilities include:

• Ensuring compliance with GDPR, CySEC rules, and DORA requirements

• Reviewing retention justifications and conducting periodic audits

• Training staff on data lifecycle management and secure deletion practices

9. Legal Basis for Processing

The Company processes personal data lawfully, fairly, and transparently in accordance with Article 6 and, where applicable, Article 9 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). All processing activities are supported by one or more lawful bases as

outlined below, depending on the nature of the data, the purpose of processing, and the relationship between the Company and the data subject.

9.1 Contractual Necessity

The Company processes personal data where it is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into such a contract. This includes processing required to: establish and maintain investment services relationships; assess applications for onboarding (e.g., KYC due diligence); provide account management and operational support; deliver services agreed upon with the client, employee, or contractor. Failure to provide such data may prevent the Company from fulfilling its contractual obligations.

9.2 Legal and Regulatory Obligations

The Company is subject to a wide range of statutory and regulatory obligations under: Law 87(I)/2017, on the provision of investment services; Law 188(I)/2007, on AML and CFT; Law 125(I)/2018, implementing the GDPR in Cyprus; Labour, tax, and social security laws, applicable to employment; CySEC directives and circulars, including DI87-01, C031, C138; Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Examples of processing under this legal basis include: client due diligence and transaction monitoring; reporting to regulatory or tax authorities; recordkeeping of investment advice or employee contracts; maintenance of internal registers, logs, and audit trails; and monitoring, classification and management of ICT-related incidents in accordance with DORA Article 9.

9.3 Legitimate Interests

The Company may process personal data where it is necessary for the purposes of its legitimate interests, provided these interests are not overridden by the fundamental rights and freedoms of the data subject. Examples include: internal administrative purposes (e.g., security monitoring, internal communications); prevention of fraud or abuse of services; defence of legal claims and litigation support; corporate governance and due diligence in business transactions; network and information systems security. Legitimate interest assessments (“LIAs”) are conducted where necessary to ensure fair balancing of interests.

9.4 Consent

In certain cases, the Company relies on the data subject’s consent to process personal data. Consent is: freely given, specific, informed, and unambiguous; collected through opt-in mechanisms or written acknowledgements; revocable at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Consent may be used for: direct marketing communications (where required by law); processing special categories of data (e.g.

biometric or health data); website cookies and tracking (via cookie banners and privacy notices). Where consent is withdrawn, the Company ceases the relevant processing unless another legal basis applies.

9.5 Vital Interests

The Company may process personal data where necessary to protect the vital interests of the data subject or another natural person, such as in medical emergencies or situations of serious safety concern. While rare, this basis may apply to: health and safety incidents involving employees or visitors; emergency disclosures to law enforcement or first responders.

9.6 Public Interest or Official Authority

In limited cases, data may be processed in the exercise of official authority or to perform a task carried out in the public interest, such as obligations stemming from regulatory inspections, whistleblowing requirements, or court orders. This legal basis is only invoked where the Company is subject to an express legal mandate.

10. How Personal Data is Collected

The Company collects personal data through multiple channels, depending on the nature of the relationship with the data subject and the context of the processing. Data may be collected directly from individuals or indirectly through third parties, as permitted by applicable data protection legislation. The Company ensures that personal data collected via ICT systems, including online platforms, mobile applications, and internal databases, complies with the requirements of the Digital Operational Resilience Act (DORA) for secure, traceable, and resilient information handling. In particular, such systems are subject to logging, real-time monitoring, and incident detection protocols to support business continuity and digital resilience.

10.1 Direct Collection from Data Subjects

The majority of personal data processed by the Company is collected directly from individuals through the following means: client onboarding forms and questionnaires submitted during account opening; Know Your Customer (KYC) and due diligence documentation, such as identification documents and proof of address; contracts and agreements, including employment contracts, service agreements, and non-disclosure agreements; applications and CVs submitted by job candidates; email communications and correspondence, including queries or service requests; telephone calls or online meetings, which may be recorded where legally permitted and disclosed in advance; website forms, including contact or subscription requests. In each case, the data subject is informed of the purpose of collection and, where applicable, is asked to provide consent.

10.2 Indirect Collection from Third Parties

In certain circumstances, the Company may collect personal data from third-party sources. These may include: publicly available sources, such as company registers, sanctions lists, or regulatory databases; regulatory authorities or supervisory bodies, as part of mandatory reporting obligations or requests; background screening and KYC service providers, who verify identity and AML-related risks; business partners, introducers, or affiliates, where personal data is shared in the context of referrals or collaborative services; group entities or outsourced service providers, performing services on behalf of the Company. Any data collected indirectly is evaluated to ensure that it is relevant, up to date, and obtained in a lawful manner. Where necessary, the Company will notify the data subject of the processing, as required by Articles 13 and 14 of the GDPR.

10.3 Automated Collection (Online Interaction)

When data subjects interact with the Company's digital platforms, personal data may be collected automatically through: cookies and tracking technologies on the website (in accordance with the Cookie Policy and applicable consent mechanisms); device identifiers and browser data, including IP addresses, device types, and language settings; usage logs, capturing activity, preferences, or error logs for system improvement and analytics. In accordance with DORA, the Company ensures that ICT systems used for automated data collection include appropriate monitoring, anomaly detection, and alert mechanisms to identify unauthorised access, cyber threats, or operational failures. This data is typically collected in anonymised or pseudonymised form, unless linked to an identified user through account registration or consent.

10.4 Updates and Changes to Personal Data

Data subjects are encouraged to inform the Company of any changes to their personal information to ensure records remain accurate and up to date. The Company may also request periodic updates as part of its ongoing due diligence or regulatory compliance procedures.

11. Use of Personal Data

The Company processes personal data strictly for lawful, specific, and legitimate purposes, as defined under the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Digital Operational Resilience Act (DORA – Regulation (EU) 2022/2554), and applicable national legislation. The processing is always conducted in accordance with the principles of fairness, transparency, data minimisation, and purpose limitation. The purposes for which personal data is used depend on the data subject category and the nature of the business relationship with the Company. Below are the main lawful bases and purposes of processing.

11.1 Contractual Necessity

The Company processes personal data when it is necessary for:

• Entering into or performing a contract with the data subject (e.g., client agreements, employment contracts)

• Delivering investment services to clients, including execution of transactions, client communication, and portfolio or account management

• Managing employment relationships, including payroll, benefits, leave, performance, and training

• Onboarding contractors or service providers, in accordance with contractual terms

This basis applies primarily to clients, employees, job applicants, service providers, and business partners.

11.2 Compliance with Legal and Regulatory Obligations

The Company is subject to various regulatory obligations under EU and Cypriot law, including those imposed by:

• Law 87(I)/2017 (MiFID II Law)

• Law 188(I)/2007 (AML Law)

• The Prudential Supervision Law (Law 165(I)/2021)

• CySEC Directives and Circulars

• DORA (Regulation (EU) 2022/2554), regarding ICT and third-party risk management

• Tax, accounting, labour, and corporate legislation

In this context, personal data may be used to:

• Conduct client due diligence (CDD) and ongoing KYC/AML monitoring

• Report suspicious transactions or submit regulatory filings to CySEC or other competent authorities

• Respond to audits, inspections, or investigations

• Maintain statutory books and employment registers

• Comply with operational resilience, ICT risk, and incident reporting requirements under DORA

11.3 Legitimate Interests of the Company

The Company may process personal data where it is necessary for the legitimate interests pursued by the Company or a third party, provided such interests are not overridden by the rights and freedoms of the data subject. Examples include:

• Monitoring and improving service quality, including customer support

• Managing risks and ensuring internal controls, such as fraud detection, IT security, and physical access control

• Enforcing contractual terms, including collection of debts or defending legal claims

• Maintaining contact with business partners, regulators, or professional advisers

• Sending client communications, subject to marketing consent rules

• Ensuring ICT system integrity, testing, and auditability in line with DORA

A legitimate interests assessment is carried out to ensure proportionality and transparency.

11.4 Consent

Where required by law or regulation, the Company relies on explicit consent to process personal data, particularly when:

• Sending direct marketing communications, newsletters, or promotional material

• Using cookies or analytics tools, in accordance with the Cookie Policy

• Processing special categories of personal data, such as health or biometric data

Consent is obtained in a clear and informed manner and may be withdrawn at any time without prejudice to the lawfulness of prior processing.

11.5 Vital Interests and Public Interest

In rare and exceptional cases, personal data may be processed to:

• Protect the vital interests of the data subject or another person (e.g., in a medical emergency or public safety context)

• Comply with legal obligations relating to public interest, such as financial crime prevention, anti-terrorism laws, operational resilience under DORA, or whistleblowing procedures

12. Legal Bases for Processing

The Company ensures that all processing of personal data is supported by a valid legal basis, as required by Article 6 and, where applicable, Article 9 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"). The Company does not engage in any processing that lacks a lawful justification. Below are the principal legal grounds on which the Company relies:

12.1 Performance of a Contract – Article 6(1)(b) GDPR

Processing is lawful when it is necessary:

• For the performance of a contract to which the data subject is a party (e.g. client agreements, employment contracts), or

• To take steps at the request of the data subject prior to entering into such a contract.

This applies to clients, employees, job applicants, service providers, and other contractual relationships.

12.2 Compliance with a Legal Obligation – Article 6(1)(c) GDPR

The Company processes personal data when required to comply with:

• Investment services legislation (e.g., MiFID II Law 87(I)/2017)

• AML/CFT obligations (Law 188(I)/2007, EU Directives, CySEC Circulars C138, etc.)

• Tax and accounting laws

• Labour laws and employment regulations

• Regulatory reporting obligations under the supervision of CySEC and other authorities

• Digital operational resilience obligations under Regulation (EU) 2022/2554 (DORA), including ICT incident reporting, risk classification, and maintaining the integrity and availability of critical data and systems

Processing under this legal basis is mandatory and continues even if consent is withdrawn.

12.3 Legitimate Interests – Article 6(1)(f) GDPR

Processing is allowed when it is necessary for the purposes of the Company's legitimate interests, provided such interests are not overridden by the data subject's rights. These may include:

• Internal governance, risk management, and compliance monitoring

• IT and system security, including incident detection and prevention

• Business continuity and client support

• Prevention of fraud and financial crime

• Legal claims and dispute resolution

• Logging and monitoring required under DORA for ICT security and continuity

A legitimate interests assessment (LIA) is carried out where required.

12.4 Consent – Article 6(1)(a) GDPR

The Company seeks explicit, freely given, informed, and unambiguous consent in the following circumstances:

• Direct marketing or promotional emails

• Use of tracking technologies (e.g. cookies), unless exempted

• Processing of certain special categories of data (see below)

Consent is always documented and may be withdrawn at any time.

12.5 Protection of Vital Interests – Article 6(1)(d) GDPR

In exceptional cases, personal data may be processed to protect the life or physical safety of the data subject or another person — for example, in a health or safety emergency.

12.6 Public Interest or Official Authority – Article 6(1)(e) GDPR

Where the Company is required to carry out tasks in the public interest (e.g. reporting under AML/CFT or DORA), this legal basis may also apply.

12.7 Processing of Special Categories of Personal Data – Article 9 GDPR

Where the Company processes sensitive data — such as health data, biometric data, or political affiliations — the processing will only occur where one of the following applies:

• Explicit consent of the data subject

• Employment or social protection law requirements

• Legal claims or regulatory purposes

• Substantial public interest, under Union or Member State law

The Company implements appropriate safeguards to protect such data, including restricted access, encryption, and policy-based access control.

13. Retention of Personal Data

The Company retains personal data only for as long as necessary to fulfil the purposes for which it was collected, or to comply with legal, regulatory, contractual, or operational requirements. Retention periods vary depending on the category of data, the nature of the processing, and the relationship with the data subject, in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007, the Law 125(I)/2018 on the Protection of Natural Persons with regard to the Processing of Personal Data, the Digital Operational Resilience Act (Regulation (EU) 2022/2554 – "DORA"), relevant CySEC Directives and Circulars, and other applicable regulatory frameworks.

13.1 General Principles

- Personal data is retained in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or further processed.

- Data is securely deleted, anonymised, or archived when no longer required, unless specific legal, regulatory, or operational obligations mandate extended retention.

- Retention periods are determined based on:

    - Applicable EU and Cyprus legislation (including AML, tax, and labour laws)

    - Statutory limitation periods for contractual, civil, or criminal claims

    - Regulatory expectations from CySEC, the Office of the Commissioner for Personal Data Protection, and other competent authorities

    - Business continuity, operational, and audit trail needs

- Digital operational resilience requirements under DORA, where data supports incident response, audit, or system recovery

13.2 Key Retention Periods by Data Category

- Customer Due Diligence (CDD) and AML/KYC Documentation: Minimum of 5 years from the end of the business relationship or the date of the last transaction (as per AML Law 188(I)/2007).

- Transaction Records and Investment Orders: At least 5 years from execution, and up to 7 years if requested by CySEC (under MiFID II and CySEC Directive DI87-01).

- Recorded Communications (e.g., emails, voice calls): Minimum of 5 years; extendable to 7 years if requested by CySEC (MiFID II requirement).

- Client Complaints and Legal Disputes: 5–7 years depending on the nature of the complaint and applicable limitation periods.

- Employment Files (including contracts, appraisals, disciplinary records): Up to 7 years after termination of employment, in accordance with labour and tax obligations.

- Recruitment Records (unsuccessful applicants): 12 months after conclusion of the recruitment process, unless further consent is obtained.

- Payroll and Tax-Related Data: At least 6 years from the end of the tax year concerned (as per tax laws).

- Marketing Data (including consent records): Up to 5 years from the last interaction or until consent is withdrawn.

- Website Usage Data and Cookies: Retained only for as long as necessary to fulfill their purpose (e.g., functionality, analytics, or security), in accordance with browser settings and the Company's Cookie Policy. Duration varies depending on technical settings and user consent preferences.

- Contracts with Third Parties, Suppliers, and Partners: Retained for at least 6 years from termination, or longer if related to disputes or audits.

- ICT-related operational data, logs, incident records, and monitoring data: Retained in accordance with DORA requirements, typically for at least 5 years, or longer where

mandated to support digital resilience, incident response, and regulatory audit trails.

13.3 Special Cases

- Legal Holds: If legal or regulatory investigations, litigation, or proceedings are ongoing or anticipated, relevant data may be retained beyond the standard retention period until formally released or the matter is resolved.

- Regulatory Audits: In cases where data is required to demonstrate compliance during inspections by CySEC, auditors, or other supervisory authorities, such records may be preserved beyond typical retention schedules.

13.4 Anonymisation and Archiving

- Where ongoing processing is no longer necessary, and legal grounds allow, personal data may be anonymised and retained for statistical analysis, operational monitoring, or internal control purposes.

- Archived data is stored securely, access is restricted to authorised personnel only, and records are clearly labelled and periodically reviewed for relevancy and risk exposure.

13.5 Review and Deletion

- The Company undertakes regular audits and reviews of all retained data, both physical and digital, to ensure that expired records are identified and removed promptly.

- When deletion is required, data is destroyed using secure, irreversible methods such as permanent deletion of digital files and cross-shredding of hard copies, in line with the Information Security Policy, GDPR, and applicable data protection and DORA requirements.

14. Security of Personal Data

The Company is committed to ensuring the confidentiality, integrity, availability, and resilience of the personal data it processes. It applies a comprehensive range of organisational and technical measures, aligned with the GDPR, the Company's Information Security Policy, and industry best practices, to safeguard personal data against unauthorised access, alteration, disclosure, or destruction. In accordance with Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), the Company also ensures the digital resilience of its Information and Communication Technology (ICT) systems used to process personal data.

Security measures are applied throughout the entire data lifecycle—from initial collection through storage, processing, transmission, and final deletion or anonymisation. These measures are continuously reviewed, assessed, and enhanced to reflect technological advancements, regulatory updates, and emerging threats.

14.1 Organisational Security Measures

The Company adopts internal policies and procedures designed to create a culture of accountability and ensure secure processing practices across departments. These include:

• Role-based access controls and segregation of duties

• Confidentiality agreements and contractual data protection clauses

• Regular training and awareness sessions for staff on data protection, phishing, password hygiene, and incident response

• Background checks during recruitment, where legally permissible and proportionate

• Appointment of a Data Protection Officer and designation of responsible personnel for data security oversight

• Secure onboarding and offboarding procedures for employees and third parties

14.2 Technical Security Measures

To protect data from internal and external risks, the Company implements a layered security infrastructure that includes:

• Firewall protection and intrusion detection systems

• Data encryption at rest and in transit using up-to-date cryptographic protocols

• Secure email gateways, anti-virus and anti-malware software

• Strong user authentication mechanisms, including password complexity and, where applicable, two-factor authentication (2FA)

• Secure backup systems with regular testing and secure offsite storage

• Use of VPNs for remote access and restricted administrative access rights

In line with DORA, the Company ensures that critical ICT systems are subject to continuous monitoring, automated alerts, and failover protocols to guarantee digital operational resilience and limit the impact of ICT-related disruptions.

14.3 Data Access and Storage Controls

Access to personal data is granted strictly on a need-to-know basis, with:

• Authorised personnel only able to access specific systems and databases relevant to their duties

• Audit trails maintained for all access and processing actions involving sensitive or critical data

• Data stored in secure servers located within the EEA or in jurisdictions offering adequate protection, with additional safeguards where required

14.4 Security in Vendor and Third-Party Relationships

The Company ensures that third-party processors and service providers handling personal data on its behalf apply security measures that meet or exceed the Company's own standards. This includes:

• Due diligence and security assessments before onboarding

• Contractual obligations to implement appropriate technical and organisational measures

• Periodic monitoring, audits, or reviews of service provider security practices

• Immediate notification requirements in the event of a breach or risk of breach

DORA obligations are reflected in third-party risk assessments, with ICT providers subject to contractual obligations for incident reporting, resilience testing, and recovery capacity.

14.5 Physical Security

Where physical storage or access is involved, the Company ensures that:

• Offices and data rooms are protected by access controls, locks, and security systems

• Physical files are stored in locked cabinets, accessible only by authorised staff

• Visitors are supervised and access to sensitive areas is restricted

14.6 Incident Response and Breach Notification

The Company maintains an Incident Response Plan for managing potential or actual data breaches. In case of a confirmed personal data breach:

• The Data Protection Officer coordinates investigation and containment

• Affected systems and data are assessed for impact and risk

• Regulatory reporting obligations under Article 33 of the GDPR are fulfilled (e.g., reporting to the Commissioner within 72 hours where applicable)

• Data subjects are notified under Article 34 GDPR if the breach poses a high risk to their rights and freedoms

• Root causes are analysed, and corrective actions are taken to prevent recurrence

In accordance with DORA, ICT-related incidents affecting data integrity, availability, or confidentiality are logged, analysed, and reported through internal and regulatory channels, with escalation protocols and digital continuity strategies in place.

14.7 Regular Monitoring and Testing

Security systems and protocols are subject to ongoing review and testing. This includes:

• Penetration testing and vulnerability assessments by internal or external experts

• Security audits and risk assessments at regular intervals

• Logging and monitoring of systems for unusual or suspicious activity

In line with DORA requirements, critical ICT assets undergo resilience testing, including scenario-based simulations, stress testing, and recovery verification, to ensure continuous data protection and business continuity. The Company's commitment to data security is embedded in its operational framework and is considered essential to the trust of its clients, partners, and regulatory stakeholders.

15. Data Subject Rights and Request Handling

The Company recognises and upholds the rights of data subjects as provided under the General Data Protection Regulation (EU) 2016/679 ("GDPR"). These rights are fundamental to ensuring transparency, accountability, and the protection of individuals' privacy. The Company also ensures that the exercise of these rights is supported by resilient ICT and data governance infrastructures, in accordance with Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector ("DORA"), particularly where rights are exercised through digital channels or systems.

All individuals whose personal data is processed by the Company, whether clients, employees, job applicants, website visitors, or third parties, are entitled to exercise specific rights in relation

to their data. The Company has implemented appropriate internal procedures to handle and respond to data subject requests in a lawful and timely manner.

15.1 Right of Access (Article 15 GDPR

Data subjects have the right to obtain confirmation as to whether the Company processes their personal data, and, where that is the case, to receive access to such data along with the following information:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the data have been or will be disclosed;
- The envisaged data retention period;
- The existence of other data subject rights;
- The right to lodge a complaint with the supervisory authority;
- Where the data were not collected directly, the source of the data;
- The existence of automated decision-making, including profiling.

15.2 Right to Rectification (Article 16 GDPR)

Data subjects may request the correction of inaccurate or incomplete personal data. The Company will verify the claim and rectify the data without undue delay.

15.3 Right to Erasure – "Right to be Forgotten" (Article 17 GDPR)

Data subjects have the right to request the deletion of their personal data in specific circumstances, including:

- Where the data are no longer necessary for the purposes for which they were collected;
- Where the data subject withdraws consent (if processing was based on consent);
- Where the data subject objects to the processing and there are no overriding legitimate grounds;

- Where the data were unlawfully processed;
- Where erasure is required to comply with a legal obligation.

The Company may refuse erasure where processing is necessary for legal compliance, public interest, or the establishment, exercise, or defence of legal claims.

15.4 Right to Restriction of Processing (Article 18 GDPR)

Data subjects may request that processing be restricted in certain circumstances, such as:

- When the accuracy of personal data is contested (for a period allowing verification);
- When processing is unlawful and the data subject opposes erasure;
- When the Company no longer needs the data but the data subject requires it for legal claims;
- When the data subject has objected to processing and verification of overriding legitimate grounds is pending.

In such cases, personal data will only be processed (except for storage) with the data subject's consent or for legal purposes.

15.5 Right to Data Portability (Article 20 GDPR)

Where processing is based on consent or contract and carried out by automated means, data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit it to another controller. This right applies only to data provided directly by the data subject.

15.6 Right to Object (Article 21 GDPR)

Data subjects may object at any time to the processing of their personal data:

- When processing is based on the Company's legitimate interests or those of a third party;
- When data are processed for direct marketing purposes.

If the objection is valid, the Company will cease processing unless it can demonstrate compelling legitimate grounds to continue.

15.7 Right to Withdraw Consent

Where processing is based on the data subject's consent, the individual has the right to withdraw that consent at any time, without affecting the lawfulness of processing carried out before the withdrawal.

15.8 Right Not to Be Subject to Automated Decision-Making (Article 22 GDPR)

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects them, unless:

- It is necessary for entering into or performance of a contract;
- It is authorised by law;
- It is based on explicit consent.

In such cases, the Company ensures human intervention, allows data subjects to express their point of view, and contests decisions where appropriate.

15.9 Exercising Your Rights and Request Handling Procedures

Requests to exercise data subject rights must be submitted in writing via the contact details provided in this Policy. The Company:

- May request identity verification before responding to the request.
- Responds without undue delay and in any event within one (1) month of receipt of the request.
- May extend the period by up to two (2) additional months for complex or multiple requests, informing the data subject of the extension and reasons.
- Will provide reasons where a request is rejected, in accordance with Article 12(4) GDPR.

These rights are provided free of charge unless the request is manifestly unfounded or excessive, in which case the Company may:

- Charge a reasonable administrative fee, or
- Refuse to act on the request.

To ensure traceability and compliance, the Company maintains a secure internal log of all data subject requests, actions taken, and response deadlines.

In line with DORA and the Company's Information Security Policy:

- All data subject rights requests are handled using access-controlled digital systems.
- Authorised personnel only are permitted to review, respond to, and record such requests.
- Communications and decisions are encrypted or securely documented to prevent unauthorised access or tampering.

16. Exercising Your Rights – Contact and Procedures

The Company is committed to ensuring that data subjects can exercise their rights in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Law 125(I)/2018, and applicable sectoral regulations, including the Digital Operational Resilience Act (DORA – Regulation (EU) 2022/2554) where ICT-related personal data is involved. The Company has established appropriate internal mechanisms to ensure secure, timely, and lawful handling of all data subject requests.

16.1 How to Submit a Request

If you wish to exercise any of your rights as described in Section 15, you may do so by contacting the Company using the contact information below:

- Email: dpo@insight.cy
- Post: IS Insight Services Ltd, Parou 6, B4, 8028, Paphos, Cyprus
- Telephone: +357 22107000

To help us process your request efficiently and securely, we may ask you to provide:

- Proof of identity (e.g. a copy of your ID or passport)
- A clear description of the data or right you are referring to
- Any relevant context or supporting documentation

All communications are protected in accordance with the Company's Information Security Policy and DORA-aligned protocols for secure communications and incident prevention.

16.2 Response Timeframe

The Company will respond to your request without undue delay and in any event within one month of receipt, in accordance with Article 12(3) GDPR. Where the request is complex or involves multiple records, the response period may be extended by up to two additional months.

In such cases, the Company will inform you within one month and explain the reason for the delay.

16.3 Limitations and Conditions

While the Company fully respects your rights, some requests may be subject to lawful limitations or exceptions. These may include:

- When data must be retained for legal or regulatory compliance (e.g. AML laws, DORA resilience logging)
- When fulfilling the request would adversely affect the rights or freedoms of other individuals
- When the request is manifestly unfounded, repetitive, or excessive

If the Company cannot fulfil a request, it will provide a clear and reasoned explanation in writing.

16.4 No Fees for Requests

The Company processes rights requests free of charge. However, where a request is clearly unfounded or excessive (e.g. repetitive without new context), a reasonable administrative fee may be charged, or the request may be refused.

16.5 Support and Assistance

If you require guidance in understanding your data protection rights or in submitting a request, you may contact the Company's Data Protection Officer (DPO). The DPO acts independently and provides support to ensure compliance with GDPR, Law 125(I)/2018, and DORA, particularly where requests concern ICT-related incidents or automated data processing environments.

17. Data Transfers to Third Countries and Safeguards

In the course of its operations, the Company may transfer personal data to third countries i.e., jurisdictions outside the European Economic Area (EEA) when such transfers are necessary for the performance of contractual obligations, the provision of services, or the use of cloud-based or outsourced solutions.

The Company ensures that all international transfers of personal data are conducted in accordance with Chapter V of the General Data Protection Regulation (EU) 2016/679

("GDPR"), the Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA), and applicable guidance from the European Data Protection Board (EDPB).

17.1 General Principles for Data Transfers

Personal data shall not be transferred to a third country or international organisation unless:

- The European Commission has issued an adequacy decision for the country, confirming an equivalent level of data protection;
- Appropriate safeguards are in place;
- The data subject has explicitly consented to the transfer, having been informed of the potential risks;
- The transfer is necessary for the performance of a contract or for the establishment, exercise, or defence of legal claims;
- The transfer is made in the vital interest of the data subject or for important reasons of public interest.

In accordance with DORA, when digital service providers (e.g., ICT third-party service providers) are located in third countries, the Company ensures that additional operational resilience and security controls are in place, particularly where such providers are critical to core functions.

17.2 Adequacy Decisions

Transfers to countries recognised by the European Commission as providing an adequate level of data protection do not require additional authorisation. The Company maintains an up-to-date list of such countries based on the Commission's official decisions.

17.3 Transfers Subject to Appropriate Safeguards

Where no adequacy decision exists, the Company may proceed with transfers only if appropriate safeguards are implemented, including but not limited to:

- Standard Contractual Clauses (SCCs) adopted by the European Commission;
- Binding Corporate Rules (BCRs) for intra-group transfers;

- Approved codes of conduct or certification mechanisms accompanied by binding and enforceable commitments;

- Ad hoc contractual clauses pre-approved by the relevant supervisory authority.

The Company also considers DORA-related obligations when engaging ICT third-party providers, ensuring that they demonstrate operational resilience, cyber risk mitigation, and business continuity capabilities.

17.4 Supplementary Measures

Where necessary, the Company may implement additional technical, contractual, or organisational safeguards to ensure that the level of data protection is essentially equivalent to that provided under the GDPR and compliant with DORA requirements. These may include:

- Data encryption and key management exclusively under EU control;

- Access limitations and audit rights over third-party processors;

- Transparency obligations and contractual warranties about government access requests;

- Assurance of digital operational resilience by the third-country provider, including incident reporting mechanisms, business continuity planning, and compliance with DORA cybersecurity expectations.

17.5 Transfers Based on Derogations

In exceptional cases, and only where none of the safeguards above are applicable, the Company may rely on the GDPR's limited derogations, such as:

- Explicit consent from the data subject;

- Transfers necessary for contract performance;

- Transfers necessary for the exercise or defence of legal claims.

Such transfers are subject to strict internal review, risk assessment, and documentation requirements, and are only used when no safer alternative is available.

17.6 Third-Party Processors and Vendors

Before engaging any third-party processor or service provider located outside the EEA, the Company:

- Conducts due diligence on the provider's data protection practices and operational resilience measures (including those required under DORA);
- Ensures that appropriate contractual clauses are signed (e.g., SCCs);
- Verifies that data access is limited to what is strictly necessary;
- Documents all assessments and transfer mechanisms used;
- Requires ICT providers to comply with incident handling, audit, and oversight requirements consistent with DORA.

17.7 Transparency and Accountability

The Company maintains a register of all international transfers of personal data and the corresponding legal basis or safeguards applied.

Data subjects may request further information regarding the safeguards in place for specific transfers, including a summary of measures adopted under DORA where ICT or critical third-party services are involved.

18. Data Breaches and Incident Response

The Company is committed to safeguarding personal data and maintaining high standards of security across its systems, in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Law 125(I)/2018, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("DORA"), and its internal Information Security Policy.

A personal data breach refers to a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Recognising that such breaches can lead to significant risks for data subjects—such as identity theft, financial loss, reputational damage, or discrimination—the Company has adopted a structured Incident Response and Breach Notification Framework.

18.1 Identification and Classification of Breaches

All employees, contractors, and external service providers are required to report any suspected or actual data breach immediately to the Information Security Officer and the Data Protection Officer (if appointed). Breaches may include:

• Loss or theft of devices or physical records

• Hacking, phishing or ransomware attacks

• Accidental or unauthorised disclosure of personal data via email or systems

• Destruction or corruption of databases

• Unauthorised access by third parties

Upon notification, the incident is promptly assessed to determine:

• The nature and scope of the breach

• The categories and volume of personal data affected

• Whether the data subjects can be identified

• The potential consequences for affected individuals

• The urgency and severity of the risk

In accordance with DORA Article 17, the Company also classifies ICT-related incidents that impact the confidentiality, integrity, or availability of personal or critical business data, including those arising from third-party service providers or ICT supply chains.

18.2 Response and Containment Measures

Once a data breach is confirmed:

• The IT and Information Security teams initiate immediate actions to contain the breach (e.g., blocking access, disabling compromised accounts, retrieving lost data, or isolating affected systems)

• The breach response team begins documenting all actions taken, including timelines and roles

• Risk mitigation measures are activated based on the Company’s Information Security Policy and Business Continuity Plan

DORA mandates that response measures be automated where feasible and that the Company maintains ICT resilience tools and recovery processes for continuity of service during incidents.

18.3 Notification to the Supervisory Authority

If the breach is likely to result in a risk to the rights and freedoms of natural persons, the Company will notify the Office of the Commissioner for Personal Data Protection (Cyprus) without undue delay and, where feasible, within 72 hours of becoming aware of it, as required by Article 33 of the GDPR.

The notification includes:

• A description of the breach and its nature

• The categories and approximate number of data subjects and records affected

• Contact details of the DPO or responsible contact person

• The likely consequences of the breach

• The remedial actions taken or proposed to address the breach

If the 72-hour window is not met, the reasons for the delay are documented and provided in the report.

In parallel, where the incident qualifies as a major ICT-related incident as defined by DORA Article 19, the Company will also notify CySEC through the designated DORA reporting framework and timelines.

18.4 Notification to Data Subjects

If the breach is likely to result in a high risk to the rights and freedoms of data subjects, the Company will notify the affected individuals without undue delay, using clear and plain language. The communication includes:

• A description of the breach and its impact

• Advice on how the individual can protect themselves

• Details of the contact person for more information

• Measures taken to mitigate the breach

Notification to data subjects may be delayed, limited, or omitted only if:

• It would hinder a criminal investigation

• Adequate technical and organisational protection measures (e.g. encryption) were in place

• Follow-up measures have rendered the risk unlikely to materialise

18.5 Documentation and Audit Trail

In accordance with Article 33(5) GDPR, the Company maintains a Breach Register that includes:

• The facts relating to each breach

• Its effects and the remedial action taken

• The justification for notification or non-notification

• Correspondence with the supervisory authority or affected data subjects

This documentation is retained for a minimum of five (5) years and is made available upon request by the supervisory authority.

Under DORA Article 20, major ICT-related incidents are subject to ongoing analysis, classification, and recordkeeping, with additional incident impact assessments and post-mortem evaluations.

18.6 Training and Awareness

The Company ensures that all employees are regularly trained on breach identification, escalation procedures, and the importance of timely reporting. Periodic simulations or drills may be conducted to test the effectiveness of the breach response plan.

DORA reinforces the requirement that staff must be continuously trained to handle ICT-related risks and to detect and report incidents in line with digital operational resilience goals.

19. Data Protection Governance and Roles

The Company recognises that a robust data protection governance framework is essential for ensuring compliance with the General Data Protection Regulation (EU) 2016/679 (“GDPR”), Law 125(I)/2018, the Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554), and the wider legal and regulatory framework applicable to investment firms in Cyprus. This section defines the internal roles and responsibilities related to data protection and digital operational resilience, ensuring clarity, accountability, and effective oversight across all processing activities.

19.1 Board of Directors

The Board of Directors holds ultimate responsibility for ensuring that data protection, digital resilience, and cybersecurity are embedded into the Company's strategy, risk management processes, and compliance obligations. Specifically, the Board: approves the Company's Privacy Policy and any material amendments; oversees the integration of data protection and digital operational resilience (as required by DORA) into operational and compliance frameworks; monitors significant data protection and ICT-related risks, receiving regular updates from Compliance and Information Security functions; ensures sufficient resources are allocated for data protection, ICT risk management, and DORA compliance.

19.2 Compliance Department

The Compliance Department is responsible for ensuring alignment of the Privacy Policy and ICT-related data processing practices with GDPR, DORA, and national data protection legislation. It monitors internal compliance with data protection policies and DORA obligations; supports business units with privacy risk assessments and documentation; conducts impact assessments (including DPIAs and DORA-mandated assessments of critical ICT functions); and coordinates with supervisory authorities including CySEC and the Office of the Commissioner for Personal Data Protection.

19.3 Information Security Officer (ISO)

The ISO ensures the technical and organisational protection of personal data and digital operational resilience under both GDPR and DORA. Responsibilities include: implementing controls to protect the confidentiality, integrity, and availability of systems; overseeing secure architecture, encryption, access controls, and monitoring systems; ensuring incident detection and response mechanisms support DORA Article 10 obligations; coordinating ICT audits and threat-led penetration testing; and working with Compliance in the event of a personal data breach or major ICT-related incident.

19.4 Department Heads and Line Managers

Departmental managers are responsible for ensuring that data protection and ICT security requirements are implemented in daily operations. They must ensure all staff understand and apply internal policies on personal data handling and ICT security; ensure data minimisation and purpose limitation are respected; and report any suspected breaches or DORA-reportable ICT incidents to the Compliance and Information Security teams without delay.

19.5 Employees and Contractors

All employees and contractors are individually accountable for protecting personal data and complying with applicable privacy and cybersecurity protocols. This includes: adhering to the Company's Privacy Policy, ICT Security Policy, and Acceptable Use Policy; participating in

mandatory training on GDPR, cybersecurity, and DORA-related requirements (e.g., reporting ICT incidents or disruptions); and immediately reporting any data breach, ICT failure, or suspected risk to the appropriate personnel.

19.6 External Data Processors and ICT Providers

Where personal data is processed or hosted by third parties, or where ICT systems are outsourced to external service providers, the Company ensures that: a written Data Processing Agreement (DPA) is in place, consistent with Article 28 GDPR and Article 28 DORA where applicable; technical and organisational measures implemented by the provider meet GDPR and DORA standards; due diligence and ICT risk assessments are conducted prior to onboarding; and ongoing monitoring and contract reviews are conducted to ensure compliance. For ICT service providers considered "critical" under DORA, the Company ensures contractual rights to audit, test, and request incident notifications in line with Articles 28–30 of the Regulation.

20. Data Protection Impact Assessments (DPIAs)

As part of its commitment to proactive data protection and operational resilience, the Company conducts Data Protection Impact Assessments (DPIAs) in accordance with Article 35 of the General Data Protection Regulation (GDPR), Law 125(I)/2018, and the DORA Regulation (EU) 2022/2554, where applicable. DPIAs are essential for identifying, assessing, and mitigating risks to the rights and freedoms of data subjects when implementing new processing operations, systems, or technologies, particularly those involving digital infrastructures.

20.1 When DPIAs Are Required

A DPIA is mandatory when a type of processing is likely to result in a high risk to individuals, particularly in the following scenarios:

• Deployment of new or emerging technologies (e.g., AI-based systems, biometric verification tools)

• Large-scale processing of special categories of data, such as health or biometric data

• Systematic and extensive profiling with legal or significant effects on individuals

• Large-scale monitoring of publicly accessible areas

• Cross-border data transfers involving sensitive or regulated data

• Use of ICT services or critical third-party providers, in accordance with DORA Article 24, where there is an impact on the security or resilience of network and information systems used for data processing

• Where required by CySEC guidance or decisions of the Commissioner for Personal Data Protection in Cyprus

20.2 DPIA Process

The DPIA process followed by the Company includes:

1. Preliminary Screening – The Compliance and Information Security Departments jointly assess whether a DPIA is required for any new project, tool, or service involving personal data.

2. Description of Processing – The relevant department documents the nature, scope, purpose, and context of processing, including ICT infrastructure and data flows.

3. Assessment of Necessity and Proportionality – The DPIA evaluates whether the processing is necessary for its intended purpose and complies with the principles of data minimisation, purpose limitation, and transparency.

4. Risk Identification and Evaluation – The Company identifies potential risks to the confidentiality, integrity, and availability of personal data, including those related to digital operational resilience (as required by DORA Articles 5 and 9).

5. Mitigation Measures – Technical and organisational measures are proposed, such as encryption, pseudonymisation, access controls, ICT continuity plans, and monitoring tools aligned with the Company's ICT Risk Management Framework under DORA.

6. Consultation and Sign-Off – DPIAs are reviewed by the Compliance Officer and, where high residual risk exists, submitted to the Data Protection Officer (DPO) and Board of Directors. Where required, the supervisory authority may be consulted.

7. Ongoing Review – DPIAs are revisited regularly, especially when there are changes to systems, vendors, risk environment, or legal/regulatory landscape (e.g., new DORA RTS/ITS or CySEC circulars).

20.3 Documentation and Retention

Each DPIA is formally documented and includes:

• A description of the processing and data types involved

• An explanation of the purpose and legal basis

• Risk identification and severity analysis

• Mitigation measures and controls

• Record of consultation with DPO, Board, or external authorities (if applicable)

DPIAs are stored securely by the Compliance Department and are available for inspection by the supervisory authority upon request. All DPIAs are retained for at least five (5) years.

20.4 Alignment with DORA Regulation

In accordance with Articles 5, 9, 24, and 30 of the DORA Regulation (EU) 2022/2554, the Company integrates digital operational resilience requirements into its DPIA process. This includes identifying ICT-related risks to data availability, ensuring third-party ICT providers meet security and data protection standards, and adopting early risk assessments for any digital transformation initiative that may affect the processing of personal data. DPIAs are also aligned with the Company's ICT risk management framework, digital continuity plans, and security monitoring systems as defined under DORA and related implementing technical standards.

21. Data Security Measures

The Company adopts and maintains robust technical and organisational measures to ensure the security, integrity, and confidentiality of personal data throughout its lifecycle, in accordance with Articles 5(1)(f) and 32 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Law 125(I)/2018, the DORA Regulation (EU) 2022/2554 on digital operational resilience, and the Company's internal Information Security Policy.

These measures are proportionate to the risks associated with data processing activities, the sensitivity of the data involved, and the potential impact on data subjects.

21.1 General Principles

The Company applies the following principles across its security and data protection framework:

- Confidentiality: Ensuring personal data is accessible only to authorised individuals;

- Integrity: Preventing unauthorised alteration or destruction of personal data;

- Availability: Ensuring data is accessible and usable when required;
- Resilience: Ensuring systems and services can withstand and recover from disruptions, as mandated by GDPR and reinforced by DORA obligations on ICT operational resilience.

21.2 Technical Measures

The Company implements the following technical security measures:

- Encryption of sensitive personal data both in transit and at rest;
- Firewalls, intrusion detection and prevention systems (IDS/IPS), and anti-malware software;
- Access controls, including password management and multi-factor authentication (MFA);
- Data loss prevention (DLP) technologies for monitoring and blocking unauthorised transfers;
- Secure system logging and monitoring of data access and network activity;
- Secure disposal of obsolete storage media and physical documents.

21.3 Organisational Measures

Organisational measures include:

- Role-based access controls and segregation of duties;
- Mandatory data protection and cybersecurity training for staff;
- Non-disclosure agreements (NDAs) with employees and external contractors;
- Documented policies for onboarding and offboarding users;
- Physical security measures, including badge-based entry, CCTV, and secure archives;
- Integration of DORA-mandated requirements for ICT risk management, incident classification, and threat-led penetration testing where applicable.

21.4 Risk Assessments and Testing

- The Company conducts periodic information security risk assessments and DPIAs;
- DORA compliance requires additional testing of ICT systems critical to service continuity, including threat scenario analysis, red-teaming, and business continuity impact assessments;
- Vulnerability scans and penetration testing are conducted regularly by qualified professionals.

21.5 Third-Party Security

- All third-party processors with access to personal data are subject to due diligence and contractual obligations;
- Data Processing Agreements (DPAs) include binding security clauses;
- Where applicable, ICT third-party risk is assessed in accordance with DORA Articles 28–41, including dependency mapping, concentration risk analysis, and termination strategies.

21.6 Business Continuity and Disaster Recovery

- A tested Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) is in place, covering both operational and data resilience;
- Backups of critical systems are encrypted and stored securely offsite;
- Restoration processes are tested periodically, with DORA-mandated response time objectives and recovery time objectives considered.

21.7 Continuous Monitoring and Compliance

- Security controls are reviewed and updated annually or following incidents or audits;
- The Company keeps up to date with developments in cybersecurity, regulatory guidance, and evolving threats;

- Internal audits and gap assessments include coverage of both GDPR and DORA compliance requirements.

The Company treats security as a fundamental part of its data governance and regulatory compliance strategy, aligning with both privacy principles and operational resilience obligations imposed by DORA.

22. Transfers of Personal Data to Third Countries or International Organisations

The Company may transfer personal data to third countries (outside the European Economic Area – "EEA") or to international organisations only where such transfers are compliant with Chapter V of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Law 125(I)/2018, and applicable provisions under the DORA Regulation (EU) 2022/2554 concerning digital operational resilience. Transfers may arise where necessary for the performance of a contract, legal obligations, or the use of external service providers including cloud-based infrastructure, ICT systems, or compliance platforms.

22.1 Lawful Grounds for International Transfers

Transfers outside the EEA may take place only where one of the following applies:

• An adequacy decision exists under Article 45 GDPR, confirming that the destination country offers adequate data protection.

• Appropriate safeguards are implemented under Article 46 GDPR, including Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or approved certification mechanisms.

• Specific derogations under Article 49 GDPR apply, such as explicit consent, performance of a contract, or legal claims.

22.2 Risk Assessment and Documentation

Before proceeding with any international data transfer, the Company:

• Conducts a Transfer Impact Assessment (TIA) in line with EDPB guidelines and DORA requirements for third-party ICT providers.

• Assesses the legal framework of the recipient country, particularly regarding access by public authorities.

• Ensures supplementary contractual, technical, and organisational measures are implemented where required.

• Documents the legal basis, destination country, safeguard mechanism, and provider due diligence in the Records of Processing Activities (ROPA) and DORA-aligned risk register.

22.3 ICT Third-Party Providers and DORA Safeguards

In accordance with Articles 28–30 and 32–33 of the DORA Regulation, the Company evaluates and monitors any third-country ICT service providers or cloud platforms involved in processing personal data. Specific safeguards include:

• Security-by-design and by-default requirements for cross-border ICT services.

• Real-time system monitoring, data access restrictions, encryption, and pseudonymisation.

• Contingency planning and exit strategies to ensure data recoverability and business continuity.

• Contractual requirements on the ICT provider to notify the Company of any access requests by foreign authorities.

22.4 Data Subject Information and Rights

Data subjects are informed about cross-border transfers in this Privacy Policy and, where applicable, at the time of data collection. They may request:

• Further details on the applicable safeguards for any international transfer.

• A copy of the Standard Contractual Clauses or BCRs used (with redactions for confidentiality reasons).

• Clarification of the Company’s risk assessment results where data is transferred to a non-adequate jurisdiction.

22.5 Oversight and Governance

All transfers are reviewed and authorised by the Compliance Department and the Data Protection Officer (DPO). In line with the DORA Regulation and GDPR accountability principle, the Company maintains a full record of all transfers and ensures regular audits, reviews, and reporting to the Board or competent authorities, where required.

23. Third-Party Processors and Data Sharing

The Company engages authorised third-party service providers ("data processors") to carry out specific data processing tasks on its behalf. These providers support critical functions such as IT operations, secure communications, compliance, payroll, CRM, regulatory reporting, and transaction execution. While these processors may access or handle personal data, they do so strictly in accordance with the Company's documented instructions and applicable legal obligations under the General Data Protection Regulation (EU) 2016/679 ("GDPR"). The Company retains full responsibility as the data controller and ensures that any processing by third parties meets the highest standards of confidentiality, security, and regulatory compliance.

23.1 Selection and Due Diligence

Before engaging any third-party processor, the Company:

• Conducts formal due diligence to assess the provider's data protection practices, security infrastructure, and legal compliance history.

• Ensures the provider has appropriate technical and organisational measures to protect personal data.

• Reviews certifications such as ISO/IEC 27001 or equivalent (where applicable).

• Evaluates risk exposure based on the type of data processed and services provided.

• Where ICT services are involved, ensures that the processor meets requirements under DORA for ICT third-party risk management and digital operational resilience.

23.2 Data Processing Agreements (DPAs)

Each processor relationship is governed by a written Data Processing Agreement (DPA) that sets out their obligations under Article 28 GDPR. These include:

• Processing data only on documented instructions from the Company.

• Implementing appropriate security measures and ensuring confidentiality of their personnel.

• Assisting in fulfilling data subject rights (e.g. access, rectification, erasure).

• Reporting personal data breaches without undue delay.

• Making available all information necessary to demonstrate compliance and allow for audits or inspections.

• Returning or securely deleting all personal data at the end of the contract.

• For ICT-related services, DPAs and related contracts comply with DORA Articles 28–30 regarding contractual requirements for ICT third-party service providers.

23.3 Categories of Processors and Services

The Company may engage processors in the following categories:

• IT and Cloud Infrastructure Providers: Hosting services, virtual servers, data storage (e.g. cloud vendors).

• CRM and Client Communication Tools: Platforms such as Bitrix24 for customer support and onboarding workflows.

• Document Management & e-Signature Services: Solutions like EBOs for secure document exchange and signing.

• Execution and Trading Platforms: Providers of STP (Straight-Through Processing) infrastructure for transaction automation and execution.

• Professional Services: External legal, accounting, audit, and tax advisors.

• HR and Payroll Providers: External firms handling salary processing, benefits, or HR documentation.

• Marketing and Website Analytics: Cookie-based tracking and website engagement tools (as covered under the Company's Cookies Policy).

• Compliance and KYC/AML Vendors: Screening platforms, sanction list databases, and automated onboarding tools.

23.4 Joint Controllers and Independent Third Parties

In limited cases, the Company may share data with third parties acting as:

• Joint Controllers, where responsibility for processing purposes and means is shared. A written arrangement defines roles and responsibilities.

• Independent Controllers, such as:

◦ Regulatory bodies (e.g. CySEC, tax or labour authorities)

◦ Courts and law enforcement agencies (in accordance with legal obligations)

◦ Banks, payment institutions, or counterparties, where required for legitimate business or AML purposes

All such sharing is limited to the minimum necessary for the intended purpose and is documented internally.

23.5 Oversight and Monitoring

• The Compliance Officer and Information Security Officer oversee third-party data processing relationships.

• The Company performs periodic reviews and assessments to verify that processors continue to meet contractual and legal obligations.

• Access to personal data is restricted to authorised personnel on a need-to-know basis.

• Any processor found to be non-compliant may be suspended or terminated, and relevant authorities may be notified if required.

• In line with DORA Articles 28–35, where ICT third-party providers are involved, the Company ensures resilience testing, performance monitoring, and exit strategies are embedded in the oversight process.

23.6 Cross-Border Data Transfers

Where a processor is located outside the European Economic Area (EEA), the Company ensures that appropriate safeguards are in place before any transfer takes place. These may include:

• Standard Contractual Clauses (SCCs) adopted by the European Commission

• Adequacy decisions for countries with recognised data protection frameworks

• Additional technical and legal protections, as required by the GDPR and case law (e.g. Schrems II).

Details of such transfers and the applicable safeguards are documented in the Company's internal records and may be made available to data subjects upon request.

24. International Data Transfers

In the course of its operations of the Company may transfer personal data to third countries i.e., jurisdictions outside the European Economic Area (EEA) or to international organisations. Such

transfers may arise in the context of service provision, use of cloud platforms, legal or regulatory obligations, or cross-border contractual relationships. All international transfers are conducted in compliance with Chapter V of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Law 125(I)/2018, and applicable guidance from the European Data Protection Board (EDPB). In line with DORA, the Company ensures that personal data collected through ICT systems is subject to security measures, real-time monitoring, and logging to support digital operational resilience, particularly for detecting and mitigating ICT-related incidents.

24.1 Legal Basis

The Company only transfers personal data outside the EEA if one or more of the following legal bases apply:

- An adequacy decision by the European Commission;
- Appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs);
- A specific derogation under Article 49 GDPR applies (e.g., explicit consent, necessity for contract performance, or legal claims).

24.2 Adequacy Decisions

Personal data may be transferred to countries that the European Commission has formally recognised as providing an adequate level of protection. In such cases, no further authorisation is required. The Company monitors and updates its list of adequacy decisions as published by the Commission.

24.3 Safeguards (SCCs, BCRs, TIAs)

When transfers are made to countries without an adequacy decision, the Company ensures the use of appropriate safeguards:

- Standard Contractual Clauses (SCCs) adopted by the European Commission;
- Binding Corporate Rules (BCRs) for intra-group transfers (if applicable);
- Approved codes of conduct or certification mechanisms, with enforceable commitments from the recipient.

Prior to transferring data under these mechanisms, the Company conducts a Transfer Impact Assessment (TIA) to evaluate the legal environment in the recipient country, including risks of government access or surveillance. Supplementary technical or organisational measures may be implemented as needed (e.g., encryption, pseudonymisation, restricted access).

24.4 Derogations

In limited cases where adequacy or safeguards are not applicable, transfers may be carried out under specific derogations set out in Article 49 GDPR, including:

- Explicit consent from the data subject, after informing them of potential risks;
- Necessity for the performance of a contract with or for the benefit of the data subject;
- Legal, regulatory, or public interest requirements, including the establishment, exercise, or defence of legal claims;
- Vital interests of the data subject or another individual (e.g., emergencies).

These derogations are used only when strictly necessary and are fully documented by the Compliance Department.

24.5 Oversight and Documentation

All international transfers are:

- Logged and documented in the Company's Records of Processing Activities (ROPA);
- Supported by a legal assessment or TIA where appropriate;
- Reviewed periodically by the Data Protection Officer (DPO) or Compliance Department;
- Subject to internal approval processes before any new cross-border processing is initiated.

Processors located outside the EEA are only engaged under written Data Processing Agreements (DPAs) that include EU-standard clauses and clearly define the scope, security measures, and compliance obligations.

24.6 Transparency for Data Subjects

Data subjects are informed about international data transfers through:

- This Privacy Policy;
- Specific privacy notices at the point of data collection;

- Contracts or service agreements (where relevant).

Upon request, data subjects may obtain:

- Further information about international transfer safeguards;
- A copy of the applicable SCCs or BCRs (with appropriate redactions for confidentiality).

25. Contacting the Company and the Data Protection Officer (DPO)

Data subjects may contact the Company for any queries or requests related to the processing of their personal data, including the exercise of their rights under the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (“DORA”). The Company provides multiple contact methods to ensure accessibility and transparency in accordance with Articles 12–15 of the GDPR and DORA Article 5(2)(b).

25.1 Company Contact Details

Data subjects can contact the Company at:

DPRG IM Ltd

Evagorou Avenue, Megaro Irene, Office 44

Lefkosia 1066, Cyprus

Tel: +357 22 322030

Email: info@dprginvestment.com

25.2 Designation of the Data Protection Officer (DPO)

In accordance with Article 37 of the GDPR, the Company has appointed an external Data Protection Officer (DPO) to independently oversee data protection compliance, handle data subject rights, and coordinate with supervisory authorities, as also aligned with the governance obligations under DORA. The DPO may be contacted for all matters related to the processing of personal data or digital operational resilience.

25.3 DPO Contact Details

IS Insight Services Ltd

Parou 6, B4, 8028, Paphos, Cyprus

Tel: +357 22107000

Email: dpo@insight.cy

25.4 Purpose of Contact and Support

The DPO acts independently and is available to assist individuals with:

- Submitting data subject requests;
- Clarifying privacy rights and processing purposes;
- Reporting security or data protection concerns, including ICT-related incidents covered under DORA;
- Initiating complaints or follow-ups with supervisory authorities.

25.5 Compliance-Related Enquiries

In addition to the DPO, the Company has appointed a dedicated Compliance Officer. The Compliance Officer operates independently from the DPO and is responsible for overseeing the Company's compliance with MiFID II, AML, and other financial regulatory obligations.

For enquiries relating to regulatory compliance, CySEC matters, or interpretation of this Privacy Policy in the context of investment services, you may contact the Compliance Officer at:

Email: compliance@dprginvestment.com

26. Version Control and Approval

This Privacy Policy is reviewed and approved by the Company's Board of Directors and is subject to periodic review to ensure ongoing compliance with applicable data protection laws, including the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Law 125(I)/2018, CySEC regulatory framework, and the Digital Operational Resilience Act (DORA).

The Company maintains version control to track amendments and ensure transparency and accountability. Any material changes are communicated internally and, where required, externally to relevant stakeholders, including clients and data subjects.

Version: 1.0

Approval Date: 14/04/2025

Approved by: Board of Directors, DPRG IM Ltd