LifeGoals.

LifeGoals Financial Services Ltd

(Regulated by the Cyprus Securities & Exchange Commission, License Number 232/14)

Policy

GDPR and Record Keeping Policy 2026

Revision history

Version	Date	Revision Author	Revision Reviewer	Revision Approver	Summary of Changes
02	24.08.2026	Roxani Ioannidou			2nd Version

Contents

1. Introduction

LifeGoals Financial Services Ltd ex. Emergo Wealth Ltd (hereinafter the "Company") was incorporated in Cyprus on 6th December 2013 as a limited liability company under the Cyprus Companies Law, Cap. 113. The Company holds a license from the Cyprus Securities and Exchange Commission (hereinafter "CySEC"), number 232/14 dated 27th March of 2014, and, further, it has obtained a license extension on 25 June 2014, which permits the Company to operate as a Cyprus Investment Firm (hereinafter "CIF") and to provide investment and ancillary services in relation to specific financial instruments.
This Policy sets out the Company's obligations of regarding data protection and the rights of Clients, vendors and employees ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. Personal Data

2.1. The following personal data may be collected, held, and processed by the Company:

2.1.1. Client Data, being personal data collected, held and processed in connection with the provision, proposed provision or termination of the Company's regulated and/or unregulated financial services to prospective, current and former clients. Client Data may include, without limitation:

(a) identification and contact information, including full name, residential and correspondence address, email address, telephone number, date and place of birth, nationality, citizenship, gender, signature, tax identification number, national identification number and social insurance number;

(b) identity-verification information, including copies and details of passports, identity cards, residence permits, driving licences and other government-issued identification documents, together with information regarding the validity and authenticity of such documents;

(c) face data and biometric information processed for identity-verification purposes, including the facial photograph contained in an identity document, a live facial photograph, video or motion capture submitted during the onboarding process, facial measurements or biometric identifiers derived from those images, and the resulting liveness, facial-similarity and identity-verification results;

(d) customer due-diligence and anti-money laundering information, including information concerning occupation, employment, business activities, source of wealth, source of funds, expected account activity, tax residency, politically exposed person status, sanctions-screening results, adverse-media findings and any enhanced due-diligence information;

(e) financial and banking information, including bank-account and IBAN details, income, assets, liabilities, investment holdings, transaction information, contribution and withdrawal information, payment records and supporting evidence concerning the origin or destination of funds;

(f) information collected for the purposes of assessing appropriateness, suitability or the provision of investment services, including the client's investment knowledge and experience, financial situation, ability to bear losses, investment objectives, risk tolerance, sustainability preferences and investment horizon;

(g) contractual, account and service information, including application forms, agreements, declarations, consents, mandates, powers of attorney, account identifiers, portfolio information, investment instructions, orders, transactions, complaints and other records relating to the services requested or provided;

(h) communications and interaction records, including correspondence, emails, telephone or video communications, recorded conversations where applicable, meeting notes, customer-service enquiries and records of instructions given to or received by the Company;

(i) technical and usage information generated through the Company's applications, websites or electronic systems, including IP address, device identifiers, login records, authentication information, operating-system information, browser information, timestamps, audit logs, security events and information concerning the use of the Company's services;

(j) information concerning authorised representatives, attorneys, trustees, directors, shareholders, beneficial owners, joint account holders, beneficiaries and other persons connected with the client or the relevant account; and

(k) any other personal data reasonably required for the Company to provide its services, administer the business relationship, safeguard its systems and assets, prevent or investigate fraud or financial crime, manage complaints or legal claims, or comply with its legal and regulatory obligations.

2.1.2. Client Data shall be collected and processed only to the extent that it is adequate, relevant and necessary for the applicable purpose and in accordance with the data-protection principles and safeguards set out in this Policy.

2.1.3. Recruiting and Hiring Data, such as name, birth date and place, address, home and professional contact details (including professional geographical or localisation data), age, gender, marital status and dependent details (for purposes of providing insurance and tax withholdings), bank details (for direct deposit of pay checks, reimbursements or bonuses), fiscal and Social Security data, citizenship/passport data, visa/permits data, and photographs (for purposes of the identification badge, organization charts, and HR performance management tools). Information relating to background checking may be collected to the extent authorized by the country of residence and the country where the employment will occur. Information relating to disabilities may be collected only to the extent that it is required by law or necessary to permit accommodations for the Personnel.

2.1.4. Employment Administration Data, such as assignment and tracking of company property assigned to the Personnel; relevant dates of career at Data Controller (entry, seniority dates, exit); job position(s); job-related privileges; business travel and expense reports; training records, work assignments, tasks, manager(s) assigned.

2.1.5. Career Advancement Data, such as education, employment history, qualification(s), competency evaluations, potential rating, evaluation of employment performance,

potential or actual promotions, changes in jobs or job titles, career path preferences and dislikes (such as possible jobs, locations), succession planning.

2.1.6. Payroll, Insurance and Benefits Data, such as wages including basic pay, recurring payments, additional payments, benefits, provision of insurance, long-term incentives, pensions, bonuses, raises.

2.1.7. Time and Attendance Data, such as work schedule, absences, attendances, overtime, substitutions, availability, absence and attendance quotas.

2.1.8. Network Security/Data Loss Prevention Data: IT communication data, such as IP addresses, email addresses (sender and recipient), email headers and content, TCP connection, user IDs, device IDs, log data, content data, date and time of data transfers.

3. Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

3.1. processed lawfully, fairly, and in a transparent manner in relation to the data subject;

3.2. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

3.4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

3.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

3.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

4.1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

4.2. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

4.3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4.4. processing is necessary to protect the vital interests of the data subject or of another natural person;

4.5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

4.6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Processed for Specified, Explicit and Legitimate Purposes

5.1. The Company collects and processes the personal data set out in Part 2 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, such as data received from employers, affiliates or partners).

5.2. The Company only processes personal data for the specific purposes set out in Part 2 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which

we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

6. Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part5, above.

7. Accuracy of Data and Keeping Data Up To Date

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Processing and Retention

8.1. The Company shall not retain personal data for longer than is necessary for the purposes for which it was collected and processed, subject to any applicable statutory, regulatory, contractual or legal record-keeping obligation.

8.2. Personal data and customer due-diligence records relating to a Client shall generally be retained throughout the duration of the business relationship and for a period of five (5) years following the termination of that business relationship, in accordance with the Company's applicable anti-money laundering, regulatory and record-keeping obligations. Financial, accounting and transactional data may be retained for a period of ten (10) years, or for such longer period as may be required or permitted under applicable tax, accounting, anti-money laundering, investment services or other legal and regulatory requirements.

8.3. The records referred to in Part 8.2 may include identification documents, identity-verification records and results, facial photographs or other material forming part of the customer due-diligence record, transaction records, communications and supporting documentation.

8.4. Where an application does not result in the establishment of a business relationship, the applicant's personal data shall generally be retained for six (6) months following the conclusion or abandonment of the application, unless a longer period is necessary for the prevention or investigation of fraud, compliance with a legal or regulatory obligation, or the establishment, exercise or defence of legal claims.

8.5. Upon expiry of the applicable retention period, personal data shall be securely deleted, destroyed or irreversibly anonymised. Electronic copies shall be securely deleted and physical records shall be destroyed using an approved confidential-destruction method.

8.6. Personal data may be retained beyond the periods specified above where:

8.6.1. retention is required by applicable law or by a competent supervisory, regulatory, law-enforcement or judicial authority;

8.6.2. the data is required in connection with an investigation, complaint, dispute or legal proceedings;

8.6.3. retention is necessary for the establishment, exercise or defence of legal claims; or

8.6.4. the Company is otherwise legally entitled or required to retain the data.

8.7. A data subject may request the deletion of their personal data in accordance with Part 15 of this Policy.

9. Secure Processing

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 20 and 21 of this Policy.

10. Accountability

10.1. The Company's data protection officer is Ms. Roxani Ioannidou; rioannidou@lifegoals.eu

10.2. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.2.1. The name and details of the Company, its data protection officer, and any applicable third party data controllers;

10.2.2. The purposes for which the Company processes personal data;

10.2.3. Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

10.2.4. Details (and categories) of any third parties that will receive personal data from the Company;

10.2.5. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.2.6. Details of how long personal data will be retained by the Company; and

10.2.7. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. The Rights of Data Subjects

11.1. The Regulation sets out the following rights applicable to data subjects:

11.1.1. The right to be informed;

11.1.2. The right of access;

11.1.3. The right to rectification;

11.1.4. The right to erasure (also known as the 'right to be forgotten');

11.1.5. The right to restrict processing;

11.1.6. The right to data portability;

11.1.7. The right to object;

11.1.8. Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1. The Company shall ensure that the following information is provided to every data subject when personal data is collected:

12.1.1. Details of the Company including, but not limited to, the identity of Ms. Roxani Ioannidou, its Data Protection Officer;

12.1.2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

12.1.3. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.1.4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.1.5. Where the personal data is to be transferred to one or more third parties, details of those parties;

12.1.6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 22 of this Policy for further details concerning such third country data transfers);

12.1.7. Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

12.1.8. Details of the data subject's rights under the Regulation;

12.1.9. Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.1.10. Details of the data subject's right to complain to the Commissioner for Personal Data Protection of the Republic of Cyprus (the 'supervisory authority' under the Regulation);

12.1.11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

12.1.12. Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2. The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1. Where the personal data is obtained from the data subject directly, at the time of collection;

12.2.2. Where the personal data is not obtained from the data subject directly (i.e. from another party):

12.2.3. If the personal data is used to communicate with the data subject, at the time of the first communication; or

12.2.4. If the personal data is to be disclosed to another party, before the personal data is disclosed; or

12.2.5. In any event, not more than one month after the time at which the Company obtains the personal data.

13. Data Subject Access

13.1. A data subject may make a subject access request ("DSR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to DSRs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2. All subject access requests received must be forwarded to Ms. Roxani Ioannidou, the Company's data protection officer, with a copy to compliance@lifegoals.eu.

13.3. The Company does not charge a fee for the handling of normal DSRs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1. If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Request for Deletion/Erasure of Personal Data

15.1. Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1. It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

15.1.2. The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3. The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

15.1.4. The personal data has been processed unlawfully;

15.1.5. The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

15.2. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3. In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1. Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1. The Company processes personal data using automated means.

17.2. Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3. Data will be provided in a structured, commonly used and machine-readable format and transmitted directly to another controller where technically feasible.

17.4. All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1. Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling) and direct marketing (including profiling).

18.2. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

18.4. Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Face Data and Biometric Processing

19.1. Categories of Face Data

19.1.1. As part of the Company's customer onboarding and identity-verification procedures, the Company may collect and process:

- the facial photograph contained in a government-issued identity document;
- a live facial photograph, video or motion capture provided by the data subject during the identity-verification process;
- facial measurements, face geometry or other biometric identifiers derived from the submitted images for the purpose of comparing the live facial capture with the photograph contained in the identity document;
- liveness, facial-similarity and fraud-detection results; and
- the outcome and supporting audit record of the identity-verification check.

19.1.2. The Company does not collect or access biometric templates used by Apple Face ID or other biometric templates stored locally on the data subject's device.

19.2. Purposes of Processing

Face data shall be collected and processed solely for the following purposes:

19.2.1. verifying that the individual completing the onboarding process is the person shown in the submitted identity document;

19.2.2. confirming that the facial capture was provided by a live person;

19.2.3. preventing impersonation, identity theft, fraud, money laundering and other financial crime;

19.2.4. conducting customer due diligence and complying with applicable legal and regulatory obligations; and

19.2.5. investigating failed verifications, suspected fraud, security incidents or attempted misuse of the Company's services.

19.3. Identity-Verification Service Provider and Sharing

19.3.1. The Company uses Onfido, an Entrust company ("Entrust"), as its identity-verification service provider. Facial captures and identity-document images are transmitted to Entrust for the performance of document-verification, facial-similarity, liveness and fraud-prevention checks on behalf of the Company.

19.3.2. Entrust may use authorised sub-processors, including cloud-hosting, technology and human-review service providers, where necessary to provide and secure the identity-verification service and subject to appropriate contractual and data-protection obligations.

19.3.3. Face data may also be disclosed:

- to competent supervisory, regulatory, law-enforcement, public or judicial authorities where disclosure is required or permitted by law;
- to authorised external auditors, legal advisers or other professional advisers where access is necessary for the performance of their duties; or

- where otherwise necessary for the establishment, exercise or defence of legal claims.

19.3.4. Face data shall not be disclosed to advertisers, advertising networks, data brokers or other third parties for their independent commercial purposes.

19.4. Storage and Security

19.4.1. Face data and identity-verification records shall be stored only within Company-approved cloud systems and the systems of authorised service providers. Any storage or transfer outside the European Economic Area shall be undertaken only in accordance with Part 22 of this Policy and applicable data-protection law.

19.4.2. Access shall be restricted to authorised personnel who require such access for customer due diligence, compliance, fraud prevention, information security or legal purposes. Appropriate technical and organisational security measures shall be applied in accordance with Parts 20 and 21 of this Policy.

20. Data Protection Measures

20.1. The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

20.1.1. All emails containing personal data may only be send at a well documented client request and must be encrypted.

20.1.2. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

20.1.3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

20.1.4. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

20.1.5. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent by via a company authorized delivery service;

20.1.6. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the department's executing manager.

20.1.7. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

20.1.8. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Ms. Roxani Ioannidou, the Company's data protection officer.

20.1.9. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

20.1.10. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

20.1.11. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the data protection officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

20.1.12. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

20.1.13. All personal data stored in the company's cloud and should not be kept on local computers or personal clouds;

20.1.14. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

20.1.15. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

21. Organisational Measures

21.1. The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

21.1.1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

21.1.2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

21.1.3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

21.1.4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

21.1.5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

21.1.6. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

21.1.7. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

21.1.8. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

21.1.9. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

22. Transferring Personal Data to a Country Outside the EEA

22.1. The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

22.2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

22.2.1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

22.2.2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Commissioner for Personal Data Protection of the Republic of Cyprus); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

22.2.3. The transfer is made with the informed consent of the relevant data subject(s).

22.2.4. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

22.2.5. The transfer is necessary for important public interest reasons;

22.2.6. The transfer is necessary for the conduct of legal claims;

22.2.7. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

22.2.8. The transfer is made from a register that, under local or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

23. Data Breach Notification

23.1. All personal data breaches must be reported immediately to the Company's data protection officer.

23.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Commissioner for Personal Data Protection of the Republic of Cyprus is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

23.3. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 23.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

23.4. Data breach notifications shall include the following information:

23.4.1. The categories and approximate number of data subjects concerned;

23.4.2. The categories and approximate number of personal data records concerned;

23.4.3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

23.4.4. The likely consequences of the breach;

23.4.5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

24. Profiling

24.1. The Company may use automated processing to evaluate certain personal aspects relating to data subjects, including their financial circumstances, investment knowledge and experience, investment objectives, risk tolerance, sustainability preferences, customer-risk classification, transaction activity, fraud risk and identity-verification results.

24.2. Profiling may be used to support customer due diligence, anti-money laundering controls, fraud prevention, appropriateness and suitability assessments, portfolio management, transaction monitoring and compliance with legal and regulatory obligations.

24.3. The Company shall ensure that profiling is conducted lawfully, fairly and transparently; uses personal data that is adequate, relevant and limited to what is necessary; incorporates measures designed to identify and correct inaccuracies; and is subject to appropriate technical and organisational safeguards.

24.4. Where profiling contributes to a decision that may produce legal effects or otherwise significantly affect a data subject, the Company shall ensure that the decision is subject to meaningful human review, unless solely automated decision-making is permitted under applicable law and the required safeguards have been implemented.

25. Automated Decision-Making

25.1. In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

25.2. The right described in Part 25.1 does not apply in the following circumstances:

25.2.1. The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject.

25.2.2. The decision is authorized by law.

25.2.3. The data subject has given their explicit consent.

26. Privacy Impacts Assessments

26.1. The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

26.1.1. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data.

26.1.2. Details of the legitimate interests being pursued by the Company.

26.1.3. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

26.1.4. An assessment of the risks posed to individual data subjects.

26.1.5. Details of the measures in place to minimize and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.