Privacy / Data Protection / Data Retention Policy

Version 6
31 January 2023

1. Introduction

Mori Capital Management Limited ("Mori", "the Company", "we", "us") is an investment management company incorporated in Malta and specialised in emerging markets. The Company is currently authorised and regulated by the Malta Financial Services Authority ("MFSA") under license number MORI-IF-10972.

Protecting the confidentiality and security of personal information is integral to the way in which Mori conducts its business. This document has been prepared pursuant to the terms of the General Data Protection Regulation ((EU) 2016/679; "GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. The GDPR does not set out any specific minimum or maximum periods for retaining personal data. Instead, companies (such as Mori) have to ensure that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, this means that the Company will:

- Review the length of time personal data is kept;
- Consider the purpose(s) the information is held for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose(s);
- Update, archive or securely delete information if it goes out of date.

Sensitive data held centrally is stored using encryption and/or password protection. Certain information is held on a need-to-know basis. This means that only required members of the Company have access to the data.

2. Data Controller

The controller of your personal data in relation to investment services provided to you and for the other purposes identified below is Mori Capital Management Ltd, with its registered office in:

Office 35
Regent House
Bisazza Street
Sliema,
SLM1604
Malta

The terms of this policy do not apply to information collected, stored, shared or distributed by third-party sites.

3. Categories of Personal Data

Mori may process the following categories of personal data:

3.1. Information Provided by You

- **Identification data and contact information:** forename(s), family name, surname, date and place of birth, nationality, personal identification number, personal ID card or passport number (name of document, number and series), place of residence (post code, town, street, building number, flat number, county, municipality), registered address, business telephone number, business e-mail address, position (including information on any political position), business name, business address, gender, photographs, IP address, tax identification number and information on tax residence status;
- **Financial and transactional data:** e.g. bank account details, money transfers, assets, declared investor profile, credit history, origin of funds, debts and expenses;
- **Data relating to your habits and preferences:** data which relate to your interest in and use of our products and services in relation with financial and transactional data;
- **Data from your interactions with us:** data collected through our internet website, meetings, calls, chats, emails, interviews, phone conversations.

3.2. Information We Receive from Other Sources

- **Information from public sources:** We may collect information from the public domain about individuals who work at companies with whom we are seeking to build a business relationship. This information typically consists of business contact details.
- **Information from our employees:** In furtherance of our employment relationship with our employees and our legal and compliance requirements, employees may provide personal information about their spouses / domestic partners and emergency contacts. Depending on the purpose, this information may include, for example, name, contact information, relationship to the employee or account information.
- **Information from our clients:** We may receive information from our clients and prospects about their personnel for purposes of enabling access to our products and managing our business relationship. This information typically consists of business contact details.

4. Purposes and Legal Grounds for Personal Data Processing

Under the GDPR, Mori is required to provide data subjects with the legal grounds or lawful basis on which the Company relies for collecting and processing personal data. The general legal grounds for processing personal data are as follows:

- Consent;
- Performance of a contract;
- Legal obligation;
- Vital interest;
- Public interest;
- Legitimate interests.

Explicit consent is required where special categories, also known as sensitive personal data, are being processed.

Typical practical examples where your personal data may be collected and processed by Mori are:

- to conclude a business agreement or any other agreement relating to the provision of investment services concluded with you;
- to take steps in order to perform an agreement relating to the provision of investment services concluded with you;
- to record transactions arising from agreements on the provision of business or investment services and for statistical purposes;
- to comply with applicable laws, rules and regulations, and in furtherance of the Company's related internal policies, including compliance polices and records retention requirements;
- to respond to your inquiries and requests that are based on legal rights that you may have (e.g., individual rights under the GDPR);
- to manage, protect against and investigate fraud, risk exposure, claims and other liabilities, including but not limited to, violations of the Company's contract terms or laws or regulations.
- to analyse customer preferences for the purpose of establishing marketing activities in which you will be interested and for conducting marketing activities regarding services provided by Mori, especially for marketing products or services that match your needs;
- to accept, review and respond to your complaints regarding Mori's activities;
- to perform the obligations imposed on the Company by the provisions of the generally applicable law;
- to perform IT management, including infrastructure management (e.g. shared platforms), business continuity and IT security;

- to establish aggregated statistics, tests and models for research and development, in order to improve the Company's risk management procedures or in order to improve existing products and services or create new ones;
- to centralise your personal data in a database enabling Company representatives to have access to it on a strict need-to-know basis, so as to allow the Company to involve the right level of expertise to deal with your requests and avoid unnecessary administrative duplications.

You need to provide your personal data to Mori to enable the Company to provide to you the services, or to comply with the obligations, referred to in this section. If there is no justification for retaining personal information, that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future. Should the Company wish to retain information about its clients or candidates in order to provide a better service to them in the future, the Company shall obtain their consent in advance

5. Processing and Sharing Personal Data

Where required by applicable data protection law, including the GDPR, the Company's processing of your personal information will be justified on a lawful basis. The Company will never sell or rent your personal information to third parties. Mori may be required to disclose your personal information for legal/compliance purposes or in connection with an investigation, or if the Company believes it is reasonably necessary to prevent harm or loss. Specifically, Mori may provide personal data to the following third parties for the purposes specified in section 4:

- entities and authorities to which the Company is obliged or authorised to provide the personal data in order to pursue the objectives specified above and for fulfilling the obligations imposed by law. This applies, in particular, to the provision of personal data to the supervisory authorities, courts and authorities (e.g. tax authorities and law enforcement authorities), independent external advisers (e.g. auditors) or entities providing services and other third parties. This also applies to entities and authorities which are authorised to receive the personal data from Mori or which are authorised to demand access to the personal data on the basis of the generally applicable provisions of the law;
- companies or persons with whom Mori has concluded a cooperation agreement on entrusting the performance of certain activities for Mori ("Data Processor"), including entities with which Mori has contracted for the destruction of data. Such entities will be obliged by the agreements they have concluded with the Company to apply appropriate security, technical and organisational measures to protect the personal data, and to process it exclusively in accordance with the instructions provided by Mori;

6. Provision of Personal Data to Third Countries

With respect to transfers originating from the European Economic Area ("EEA") to the United States and other non-EEA jurisdictions, where the level of protection has not been recognised as adequate by the European Commission, we implement standard contractual clauses approved by the European Commission and other appropriate solutions to address cross-border transfers, as required or permitted by Articles 46 and 49 of the GDPR.

7. Period of Personal Data Storage

The Company's standard operating procedure is to retain your personal information for the period during which Mori has a relationship with you. However, there are many reasons why the Company may need to retain your data for longer. For example, the Company may need to retain your personal data if the purpose for which it was collected extends beyond the term of the business relationship. The Company may also retain your personal information for a term that corresponds to a statute of limitations, to establish, exercise or defend legal claims, or as otherwise permitted or required by law, so that in each case the Company has an accurate record of your dealings with us in the event of any complaints or challenges. The Company may also retain your personal information for compliance or regulatory purposes, where the Company is required to do so in accordance with legal, tax and/or accounting requirements, or to support a legal process, audits or requests, or requirements of a legal authority or other governmental entity having authority to make the request.

8. Rights of Data Subjects

Depending on the objective and the grounds on which Mori processes your data, you may be entitled to the following rights regarding Personal Data protection:

- right to access your personal data: the data subject is authorised to obtain confirmation from Mori as to whether that person's personal data is being processed and, if so, he/she is authorised to obtain access to it. Mori shall provide you with a copy of the personal data that is being processed at your request. Mori may collect a charge at a reasonable amount arising from the administrative costs for all further copies which you request;
- right to rectify your personal data: you are entitled to correct the personal data which applies to you and which is incorrect. Subject to the objectives of the processing, you are entitled to request that incomplete personal data is supplemented, including by presenting an additional declaration;

- right to erase your personal data: you are entitled to demand the deletion of your personal data if the circumstances provided for by law take place. In such a case, Mori shall delete such personal data without delay;
- right to restrict processing of your personal data: in such a case, Mori shall, at your request, specify that data and it may only be processed for specified purposes;
- right to data portability: under certain circumstances, you are entitled to receive your personal data in a structured, commonly used machine-readable format, which has been provided to Mori, and you are entitled to send this personal data to another entity without obstruction by Mori;
- right to object to further processing of your personal data: in certain circumstances, you are entitled to file an objection to the processing of your personal data for reasons related to your particular situation, and Mori may be required to stop processing such personal data;
- right to file a complaint with the appropriate supervisory authority if the data processing breaches the provisions of the GDPR.

9. Types of Information

This section explains the differences among records, disposable information and personal data belonging to others

9.1. Records

A record is any type of information created, received or transmitted in the transaction of Mori's business, regardless of physical format. Examples of where the various types of information are located are:

- Appointment books and calendars.
- Audio and video recordings.
- Photographs.
- Computer programs.
- Contracts.
- Electronic files.
- E-mails.
- Handwritten notes.
- Invoices.
- Letters and other correspondence.
- Magnetic tape.
- Memory in mobile phones and PDAs.
- Voicemails.

9.2. Disposable Information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders and other printed materials obtained from sources outside of Mori and retained primarily for reference purposes.
- Spam and junk mail.

9.3. Personal Data

Personal data is defined as any data which the Company possesses and which can identify an individual either on its own or when combined with other data. Some examples of personal data include names and addresses, email addresses, CVs, details of previous employment, medical records and references. Mori is bound by the specific obligations relating to personal data as set out in the GDPR.

10. Records / Data Retention and Destruction

Any physical records and electronic files that are part of any of the categories listed in the Records Retention Schedule contained in the annex to this policy, must be retained for the amount of time indicated in it. A record must not be retained beyond the period indicated in the Record Retention Schedule unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention.

Physical documents will be destroyed by shredding after they have been retained until the end of the document retention schedule. Electronically stored data will be erased after they have been retained until the end of the document retention schedule. The media used to store this data, such as hard disks or USB storage units or DVDs, will be physically destroyed at the time of their decommissioning.

11. Data Security and Breach Reporting

While Mori is committed to safeguarding and protecting your personal information from unauthorised access, improper use or disclosure, unauthorised modification or unlawful destruction or accidental loss, and Mori utilises and maintains certain reasonable processes, systems, and technologies to do

so, you acknowledge that no transmission over the Internet is completely secure or error-free, and that these processes, systems and technologies utilised and maintained by Mori may be subject to compromise. Accordingly, the Company cannot be held responsible for unauthorised or unintended access that is beyond the Company's control.

Hardcopies of documents pertaining to any of the categories listed in the Records Retention Schedule will be kept securely onsite in a locked cabinet or a similarly secured arrangement until destruction. If off-site document scanning of hardcopies is required, they will be transferred securely to the off-site location, where they will be stored securely (if required) and returned promptly.

GDPR requires controllers to notify any personal data breach to the applicable regulator and, in certain instances, the data subject, within 72 hours of having become aware of the breach. The Company has put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where the Company is legally required to do so. If any client or employee becomes aware or suspects that a personal data breach has occurred, they should immediately contact the Company or, in case of staff members, the person or team designated as the key point of contact for personal data breaches. Timely reporting is essential because of the stringent requirements under the GDPR for reporting breaches. Clients/Investors should preserve all evidence relating to the potential personal data breach.

A personal data breach is any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that Mori, or any of the Company's third-party service providers, put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

12. Contact

Should you wish to exercise any of your GDPR rights, or for any questions in relation to this policy, please contact Mori at:

Mori Capital Management Limited
Office 35, Regent House
Bisazza Street
Sliema - SLM 1604
Malta
Email: info@mori-capital.com

13. Changes to this Policy

The wording of this policy may be changed from time to time to reflect changes in Mori's practices concerning the collection and use of personal information.

ANNEX - Records Retention Schedule

Staff Records	
Record	**Retention Period**
Benefits description for employee	6 years from when the record was required to be disclosed
Employee applications and resumés	6 years or, where successful, for the duration of the employment plus 7 years from the date of termination of employment
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training)	6 years from the data of making record or action involved, whichever is later, or 1 year from data of involuntary termination
Records relating to background checks on employees	6 years from when the background check is conducted
Employment contracts; employment and termination agreements	7 years from the date of expiry of the contract or agreement
Employee records with information on salary rates	6 years
Injury and illness incident reports and related annual summaries; logs of work-related injuries and illnesses	6 years
Job descriptions, performance goals and reviews	For the duration of the employment plus 7 years from the date of termination of employment
Personnel or employment records	6 years from the date the record was made
Training agreements, summaries of applicants' qualifications, job criteria, interview records	Duration of training + 4 years
Client Records	
Client personal details / Client business details / Client related transactional details	At least for the duration of the business relationship. Potentially longer subject to regulatory / legal obligations.
Candidate Records	
Candidate CVs	For the duration of the relationship with the Company
Corporate Records	
Articles of incorporation / Bylaws	Permanent
Annual corporate filings	Permanent
Board policies, resolutions, meeting minutes and committee meeting minutes	Permanent
Contracts	Permanent
Business e-mails	6 years
Tax records	Permanent
Sales and purchase records	6 years
Accounting & Finance	
Accounts payable and receivables, ledgers and schedules	7 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	2 years
Business expense records	7 years
Electronic fund transfer documents	7 years
Invoices	7 years