DMA Mauritius Data Retention and information sharing Policy

(the "Policy")

1. Introduction

The purpose of this policy is:

- To ensure compliance with all legislation applicable to the retention of data.
- To provide guidance as to how DMA treats its documents, records and other data, including client, lead and employee data and furthermore how it treats such data which it processes on behalf of other group offices.
- To give DMA employees direction and rules to be used when making a decision on whether specific data should be retained, including for how long or whether it should be destroyed.
- To give DMA employees direction and rules on what data can be transferred to/ shared with other offices within the DMA Group and/or to third parties.

The latest edition of this document is at all times found on the intranet under Policies & Procedures.

This policy applies to DMA and any data processed by DMA on behalf of the DMA Group which includes SCM DMA (Pty) Ltd (South Africa).

2. Legal requirements

a. The Data Protection Act 2004

DMA is obliged to comply with The Data Protection Act 2004 which is largely based on Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and the free movement of such data. The Act applies to all information processed electronically and in physical records, which can be assigned to an identified or identifiable person. In DMA this will include information on clients, leads and employees. When handling such data, DMA must comply with best practice for handling of personal data. This implies that all handling of data must be reasonable in proportion to the purpose of the data collection. For that reason, collection of data must be done for explicitly stated objectives, and future processing of the data must be in accordance with previously stated objectives. Should stored information turn out to be incorrect or misleading, e.g. by mixing up two persons in case of name similarity, said information should be deleted.

b. Information to be given to clients

When collecting information regarding a person, the person should be provided with the following information:

1) The identity of the company processing the data (i.e. DMA)
2) The purpose of the processing for which the data is intended
3) any further information which is necessary, having regard to the specific circumstances in which the personal data are collected, to enable the data subject to safeguard his or her interests, such as:
   (a) the categories of recipients;

(b) whether replies to the questions are obligatory or voluntary, as well as possible consequences of failure to reply;
(c) the rules in relation to the right of access to and the right to rectify the data relating to the data subject.

c. Processing of data – client consent to disclose information

Processing of personal data is subject to strict measures. As point of departure, personal data obtained must never be disclosed to a third party unless the client has given his/her explicit consent. As all entities in the DMA Group are considered to be third parties, disclosure of client information to other entities within the Group is contingent on the client's consent. Whenever there is a need to share client information with third parties, be it other entities in the Group or data providers, the relevant business owner shall ensure that the clients have consented to the transfer of the client information prior to the transfer. Personal data may be disclosed to a third party without consent if there is a legal requirement to do so (e.g. in cases of suspicion of money laundering). Furthermore, usual client information which includes, but is not limited to, name, address, social security number, account status, name of instruments, margins etc., may be transferred to a third party without client consent where legislation and or regulation allows for same. Where information is disclosed to a service provider, the service provider is subject to the identical confidentiality obligations as DMA.

When signing the Client Application Form and the General Business Terms, the client should give his consent to the following:

- Legal requirements: That DMA can disclose client information to a third party if DMA is obliged hereto due to prevailing legislation, or to a legislative or supervising authority, or to another person who according to the law is entitled to demand disclosure, or in order to sufficiently fulfill its obligations pursuant to the Terms. This can be done without prior notice to the client.
- Disclosure within the DMA Group: That personal information including name, personal identification number, address etc., as well as client information including account information, entries, investments etc., may be disclosed within the DMA Group for the purpose of conducting risk management, providing trade recommendations, trading activities, sales and marketing information including new products and services.
- Disclosure to third parties: That personal information may be shared with a third-party agency working on behalf of DMA Group with the purpose of performing client analysis for the use of DMA Group's sale and marketing.
- Completion of due diligence: That DMA may share information with any introducing broker for the purpose of completing the due diligence and approving of account applications.
- Third party authentication service providers: That DMA may share information with a third-party authentication service provider for the purposes of verifying the client's identity and that a record of the search will be retained.
- Recording of telephone conversations, internet conversations and meetings: That DMA may record all telephone conversations, internet conversations, and meetings between the client and DMA, and use such recordings, or transcripts from such recordings, as evidence towards any party to whom DMA, at its reasonable discretion, sees it to be desirable or necessary to disclose such information in any dispute or anticipated dispute

d. Processing of data – lead consent to disclose information

When a lead signs up e.g. for a demo account, the lead consents to DMA, or anyone in the DMA Group being allowed to contact the lead via phone or email, with information on products and services, and to assist the lead in using any of the DMA Group offerings.

Information on leads cannot be retained longer than what is needed for the purpose. If a lead becomes a client the information must be assessed as client documentation. If the lead does not become a client, e.g. by not funding his/her account, the information must be deleted when establishment of a contractual relationship with the lead is assessed unlikely.

e. The client's/ lead's right to access data

Upon request from a client/ lead, DMA is obliged to provide information regarding whether the DMA is processing data relating to the client/ lead. Where such data are being processed, the client/ lead shall be informed about:

- the data which are being processed
- the purpose of the processing
- the categories of recipients of the data; and
- available information on the source of such data

As there can be exceptions to the above, please contact Compliance in case a client/ lead requests information regarding the processing of his data. Compliance will then assess whether said information should be given to the client/ lead.

f. Transferring of data

In terms of data protection, The Data Protection Act distinguishes between safe countries with an adequate level of protection and countries with an inadequate level of protection. As all countries within the European Union are covered by Directive 95/46/EC, and hence apply the same level of protection, all EU countries (and EEA countries) are considered to have an adequate level of protection.

The adequacy of the level of protection ensured by countries outside the European Union is assessed by the European Commission, among other things on the basis of the country's legislation. The European Commission has already recognized that the following countries provide an adequate level of protection: Andorra, Australia, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Faeroe Islands, Israel, New Zealand and Uruguay. For additional information or for the most recent updates of the list of countries ensuring an adequate level of protection, consult the European Commission's website. Note

that the "Safe Harbor" arrangement previously applicable for data transfer arrangements with entities located in the USA is currently invalid.

As point of departure, DMA is not allowed to transfer any data outside the DMA Group to third parties resident in countries without an adequate level of data protection ("Third Countries"), in accordance with Section 27 (1), i.e. countries outside the EU/EEA, which are not on the Commission's list of "safe" countries, cf. above. The term "third party" includes third party companies processing data on behalf of DMA from a location in an "unsecure" country, i.e. for marketing or outsourcing purposes.

Transfer of data to a party located in a Third Country will require either an explicit consent from the client to the transfer or, alternatively, that DMA and the third party sign a Contract that requires compliance with the Data Protection Act.

DMA will always ensure that Client Data is adequately protected and only used as agreed/consented to.

g. Incorporation of Standard Contractual Clauses

Despite the fact that the client gives consent to disclosure of information within the DMA Group and in regards to processing of data by a third party in connection with marketing analysis etc., incorporating appropriate contractual clauses into a contract with third party providers to comply with requisite Data Protection legislation and regulation will allow for personal data to flow from a Data Controller established in any Mauritian and/or EU/EEA country to a third party established in a country not ensuring an adequate level of data protection (where necessary), as incorporation of the contractual clauses commits the third party to comply with standard data regulation.

h. Cloud Computing

The use of Cloud Computing is gaining ground around the world, but it is important to observe the data regulation before entering into an agreement with a supplier. Before entering into an agreement it should be ensured that adequate data safety measures, such as encryption and segregation of data, are in place. Furthermore, it should be considered what types of data are being transferred (client data/lead data, personal information vs. non personal information, the objective, e.g. marketing or administration, etc.). Compliance should always be consulted in such cases.

i. Employee documents

Employee documents are all documents relating to the contractual relationship between the employee and DMA, such as job applications, contracts and other files. Information such as name, address, phone number, birthday, close family, education, CV, salary, sickness absence etc., are considered "usual information". Such information can be retained, to the extent DMA needs them.

As a rule, DMA may retain information related to an employee, which the employee submits in his/her job application. These employee documents must be retained for 5 years after the employee has terminated the employment with DMA. When the information has been retained for 5 years it must be destroyed. The documents and data can be retained as physical documents and/or in electronic form.

Retention of sensitive information such as e.g. health information regarding abuse of alcohol, crime, race/ ethnic background, religion etc., may, as a main rule, only be retained if the employee has given explicit consent. However, should retention of sensitive information be necessary in order to comply with existing laws, an exception from above mentioned rule, can be made.

j. Job applications, CV's, etc. related to non DMA employees

Job applications and related documents such as CV's are stored for 6 months in DMA's database. Data within the database may be used for anonymous statistics. The information will be used collectively and no individual users of the database can be identified based on the information used. Should an applicant want his/ her application to be erased from the database before the storage period expires, the applicant shall instruct DMA to erase the data from the database. When an applicant submits an application, he/ she agrees to the above.

When an applicant uploads his/ her CV to DMA's database, the CV will be deleted 6 months after it was uploaded or previously updated.

k. Act on Measures to Prevent Money Laundering and Financing of Terrorism

In accordance with legislation and regulation on Measures to Prevent Money Laundering and Financing of Terrorism, DMA shall store client's personal data for five years after the client relationship has been terminated and the client account is without funds. No later than five years and one month after the termination and withdrawal of all client funds the personal data shall be deleted.

Identity documents obtained pursuant to the customer due diligence section in in respect of relevant legislation and regulation on Measures to Prevent Money Laundering and Financing of Terrorism are encompassed by above retention period. Included are account opening documents such as passport copies (proof of identity), address information (proof of residency), ownership documents, information regarding beneficial owners, information on the objective and intended nature and extent of the business relationship, etc.

As this retention is required by law, clients and beneficial owners of corporate clients will not need to give consent to the retention of their identification documents.

Additionally, documents and records containing information regarding trades and transactions shall be stored for a minimum of 5 years after execution of a transfer and shall be deleted no later than five years and one month after the transaction has been executed. This also applies to information regarding suspicious transactions, when DMA deems there is an increased risk of money laundering or terrorist

financing, e.g. due to the size or pattern of the transaction(s) or because of a connection to a country where the FATF has deemed the risk of money laundering or terrorist financing to be increased.

In accordance with legislation and regulation on Measures to Prevent Money Laundering and Financing of Terrorism, DMA is obliged to exchange information within the DMA Group regarding notification of clients to the authorities with the purpose of fighting money laundering and terror financing. The process for exchanging information is further described in a procedure.

3. Data categories covered by this policy

Listed below are a number of document and data retention groups. The groups reflect the different practical, security and legal requirements, which apply.

Category	Description	Retaining period
Client documents and data	Client information, including debit and credit card data, must be retained for 5 years after the end of the client relationship. The client relationship ends when the client terminates the relationship, or if for some reason DMA terminates the client relationship, and there are no more client funds on the account. When the information has been retained for 5 years it must be destroyed no later than five years and one month.	5 years*
Personal information accrued to DMA	Included is information on leads. Information on leads is data which can be referred to an individual, who is not a client, thus the information cannot be retained longer than what is needed for the purpose. This means that if the lead becomes a client the information must be assessed as client documentation, c.f. above. Further, if the lead does not become a client, e.g. by not funding his account, the information must be deleted once we are able to assess that a contractual relationship is undesirable. Included is also information as job applications, CVs etc. which do not result in the applicant becoming a DMA employee. This information can be referred to an individual, thus it must not be retained longer than what is needed for the purpose. If the applicant does not wish to be kept in our database, his application will be deleted as soon as the vacant job has been occupied. Should the applicant wish to be stored in our database, the data will be stored for 6 months. If the applicant becomes a DMA employee the documents relating to the employee must be treated as individual employee human resources documents	No longer than what is needed for the purpose

Category	Description	Retaining period
	and data. Special rules may apply for employees of branch offices according to local regulations.	
Employees - Human Resources documents and data	Employee documents are all documents relating to the contractual relationship between the individual DMA Employees and DMA. It is such material as employee applications, contracts and files. These employee documents must be retained for 5 years after the employee has terminated the employment with DMA. When the information has been retained for 5 years it must be destroyed. The documents and data can be retained as physical documents and/or in electronic form. Special rules may apply for employees of branch offices according to local regulations.	5 years
Accounting documents and data	Accountancy documents and data must be retained for 5 years following the end of the financial year to which the documents and data refer. When the information has been retained for 5 years it can be destroyed.	5 years
Reports and statements	Financial reports, management reports and compliance reports and statements including yearly statements which are not covered by other data groups should be kept as long as the data owner deems it necessary but for at least 5 years.	5 years
Business transaction records	This includes all documents and data relating to agreements on business transactions with partners and clients which can have legal regulatory and operational impact. Records of client transactions must be retained for 5 years after the transaction has been recorded.	5 years
Security Audit Trails	Security audit trails and event log data maintain a record of system activity by system or application processes and by user activity. Some elements or events of these logs can be relevant to business transactions. These elements and events should be defined and kept in and together with the business transaction records. Therefore the retention of these records can be independent from business transaction records. The records must be retained for at least 1 year.	At least 1 year Recommended 5 years

Category	Description	Retaining period
IT configuration data and related information	Information related to the DMA's Configuration Items must be stored to document significant events and allow for forensic investigations. The relevant information is mainly stored in DMA's CMDB, including master data of IT components (hardware and software configurations, etc.) as well as related work items (changes, incidents, problems, etc.).	At least 3 years Recommended 5 years (online or offline)
Documents and Data not covered by the Document and Data Retention Groups	Documents not covered by above mentioned categories must be retained according to the operational needs of DMA, the applicable legislation, security standards and practical measures. As a general rule of thumb all business related documents and data must be kept for five years and all documents and data related to individuals, e.g. clients must be destroyed if there is no longer a valid reason to keep it. If you are in doubt do not hesitate to contact Compliance who will assess the retention time of the particular document or data.	General rule – 5 years
Electronic Communications	All e-mails and landline/ IP phone calls (incoming and outgoing) must be retained.	No longer than what is needed for the purpose

4. Responsibilities

Function	Responsibility
Board of Directors	• Responsible for ensuring compliance with the provisions of the law.
Management	• Ensure effective daily management of DMA's data handling and protection of data. • Responsible for establishing and communicating data and information security policies and for ensuring that they are observed. • Ensuring that appropriate action is taken if it appears that the sufficient data protection is not carried out and that procedures function effectively and in compliance with applicable laws and regulatory requirements. The Board of

Function	Responsibility
	Management must report any actions taken to the Board of Directors immediately.
Group IT	• Implementing relevant data and system protection according to this policy and DMA's Information Security Policy. • Monitoring and executing relevant data and system protection controls according to this policy and the Information Security Policy.
Group Compliance	• Identification, analysis and management of risks related to data and system protection, storing, disclosure and destroying. • Development of appropriate policies, procedures, standards and guidelines in line with legal regulatory requirements • Support the implementation and understanding of relevant policies and guidelines for example through awareness, reviews, etc. for all relevant parties • Reviewing and maintaining DMA's Data Retention and Information Sharing Policy. • Monitor and inform relevant people and departments about changes in legislation relevant to this policy. • Advise the Board of Directors, Management and other functions on the scope of this Data, Document and Information sharing Policy and the relevant rules. • Report promptly to Management on any material failures according to this policy accurse. • Advising business on the policy whenever questions may occur.
All employees	• All employees, who use the data in their function, as described in this policy, must comply with this policy. This means that all employees are responsible for ensuring that the data is treated according to the policy, including treating the data in accordance with the Data categories, - see section 3. • To inform Legal & Compliance whenever significant changes occur which can affect the content of the policy. • Archive paper documents by physical storage. Paper documents can also be retained by scanning. When documents are scanned it is important to consider whether the original paper documents should be destroyed or stored physically. If in doubt contact Compliance. Further data can be retained in electronic form, e.g. e-mails, in CRM, as MS Office files, in PDF-format files etc. • Document and Data shall be protected, stored, disclosed and destroyed in accordance with DMA's Information Security Policy
System owners	• That data related to the system they are classified as owners for are protected, stored, disclosed and destroyed according to this policy and requirements in DMA's Information Security Policy • When Compliance informs about changes in legislation - follow up on and implement relevant changes.

5. Non-compliance consequences

Being in non-compliance with the policy can potentially entail these consequences for DMA, e.g.:

- Operational problems
- Failure to comply with legislation, including difficulty in defending legitimate claims
- Lack of evidence and audit trails in case of disputes
- Loss of reputation, hence loss of business opportunities
- Inspections by the FSC or other regulatory authority leading to sanctions (civil and/or criminal)

6. Risk and incident reporting including escalation

Any breaches of this Policy should be reported to Compliance who must escalate the matter immediately to the relevant Department Head. Questions related to this Policy should be directed to Compliance.

7. Business continuity

In case of IT-system deficiencies, duties described in this Policy should be postponed until system access and functionality is re-established.

8. Data Protection and Privacy Policy Statement

The following shall be disclosed on our website:

Your Personal Information

This Data Protection and Privacy Statement relates solely to information supplied by you on this Website. SCM DMA (Mauritius) Limited, the Data Controller ("DMA") respects the privacy of your personal information and will treat it confidentially and securely.

Any personal information provided by you to DMA through this Website or through one of the Trading Portal's offered to you by DMA will be used for the purpose of providing and operating the products and services you have requested at the Website or Portal and for other related purposes which may include updating and enhancing DMA's records, understanding your financial needs, advising you of other products and services which may be of interest to you, for crime/fraud prevention and debt collection purposes, for purposes required by law or regulation, and to plan, conduct and monitor DMA's business. The information collected from you by DMA will be valuable in improving the design and marketing of our range of services and related products for customer use. This Policy will not alter or affect any information otherwise provided by you to DMA.

Other than to those individuals and entities listed below your details will not be revealed by DMA to any external body, unless DMA has your permission, or is under either a legal obligation or any other duty to do so. For the purposes detailed above, your information may be disclosed to:

- *other Branches or Companies in the DMA Group (ie. DMA, its subsidiaries, affiliates and parents);*
- *any regulatory, supervisory, governmental or quasi-governmental authority with jurisdiction over the DMA Group;*

- *any agent, contractor or third-party service provider, professional adviser or any other person under a duty of confidentiality to the DMA Group;*
- *credit reference agencies and, in the event of default, debt collection agencies;*
- *any actual or potential participant or sub-participant in, assignee, novatee or transferee of, any of the DMA Group's rights and/or obligations in relation to you;*
- *any financial institution with which DMA has or proposes to have dealings.*

The above disclosures may require the transfer of your information to parties located in countries that do not offer the same level of data protection as your home country. However, DMA will ensure that parties to whom your details are transferred treat your information securely and confidentially. DMA also pledges its intention fully to meet any internationally recognised standards of personal data privacy protection and to comply with applicable data protection and privacy laws. We may transfer your information if it is necessary to perform our contract with you and by providing details to DMA via this Web Site or the Portal you are deemed to consent to any other transfers.
Information held about you is retained as long as the purpose for which the information was collected continues. The information is then destroyed unless its retention is required to satisfy legal, regulatory or accounting requirements or to protect DMA's interests. As a general rule, the maximum retention period is 7 years.

It is your responsibility to maintain the secrecy of any user ID and login password you hold.

9. Cookies

In order to improve our Internet service to you, we will occasionally use a "cookie" and/or other similar files or programs which may place certain information on your computer's hard drive when you visit an DMA website. A cookie is a small amount of data that our web server sends to your web browser when you visit certain parts of our site. We may use cookies to:

- *allow us to recognise the PC you are using when you return to our website so that we can understand your interest in our website and tailor its content and advertisements to match your interests (This type of cookie may be stored permanently on your PC but does not contain any information that can identify you personally.);*
- *identify you after you have logged in by storing a temporary reference number in the cookie so that our web server can conduct a dialogue with you while simultaneously dealing with other customers. (Your browser keeps this type of cookie until you log off or close down your browser when these types of cookie are normally deleted. No other information is stored in this type of cookie.);*
- *allow you to carry information across pages of our site and avoid having to re-enter that information;*
- *allow you access to stored information if you register for any of our on-line services;*
- *enable us to produce statistical information (anonymous) which helps us to improve the structure and content of our web site;*
- *enable us to evaluate the effectiveness of our advertising and promotions.*

Cookies do not enable us to gather personal information about you unless you give the information to our server. Most Internet browser software allows the blocking of all cookies or enables you to receive a warning before a cookie is stored. For further information, please refer to your Internet browser software instructions or help screen.

10. *Internet and Telephonic Communications*

In order to maintain the security of our systems, protect our staff, record transactions, and, in certain circumstances, to prevent and detect crime or unauthorised activities, DMA reserves the right to monitor all internet communications including web and email traffic into and out of its domains. DMA maintains recorded telephone lines.

11. *Your Rights and How to Contact Us*

You may have the right under data protection legislation on payment of a fee to request access to personal information about you held by us and to have it corrected where appropriate. If you have that right and you wish to access, correct or delete any of your personal data held by us, or if you have any questions concerning our Data Protection and Privacy Statement please contact the relevant DMA Data Protection representative. You may also have the right to access details held by credit reference agencies and DMA will supply details of the relevant agencies upon request. Kindly contact the DMA offices who will direct your call accordingly.

12. *Contacting You*

In providing your telephone, facsimile number, postal and e-mail address or similar details, you agree that DMA may contact you by these methods to keep you informed about DMA products and services or for any other reason. If you prefer not to be kept informed of DMA products and services, please contact DMA telephonically per above.

DMA reserves the right to amend its prevailing Data Protection and Privacy Statement at any time and will place any such amendments on this Website. This Data Protection and Privacy Statement is not intended to, nor does it, create any contractual rights whatsoever or any other legal rights, nor does it create any obligations on DMA in respect of any other party or on behalf of any party.