DATA PROTECTION POLICY

		Date: 06/12/2022
Owner: Alexandre Hecklen	**Reviewed by:** **Diego Ofano**	Replacing the Policy dated on 16/02/2021

Index:

1. CONTENT

1.1. Legal background

This Policy provides for the principles and measures adopted by the MC Square S.A (hereinafter "MC Square" or "the Company") based on the following European Union and Luxembourg laws and regulations, including without limitation:

- Regulation EU 2016/679 – General Data Protection Regulation- "GDPR";
- Directive 2002/58/EC on Privacy and electronic communications;
- Law of August 2nd,2002 on the protection of individuals with regard to the processing of personal data amended from time to time;
- Law of May 30th, 2005 - laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector;
- The CSSF Circular No. 18/698 regarding the authorisation and organisation of investment fund managers incorporated under Luxembourg law and specific provisions on the fight against money laundering and terrorist financing applicable to investment fund managers and entities carrying out the activity of registrar agent.

Following the global pandemic of the COVID-19 and the measures put in place in order to face that pandemic, the European Commission has adopted:

- The Recommendations EU 2020/518 as of 08 April 2020 in order to facilitate and monitor the use of digital technologies and data in response to the current crisis.

All terms in capital letters unless otherwise defined in this Policy shall have the meaning given by GDPR.

1.2. Purpose

This Policy lays down the principles to which employees must adhere to guarantee confidentiality and professionalism in activities involved in Personal Data Processing in compliance with the applicable legal provisions.

The Policy sets forth:

- The principles and obligations of the Data Controller regarding Processing of the Personal Data;
- The rights of the Data Subject whose Personal Data is processed;
- The various types of Personal Data Processing;
- The principles of transfers of Personal Data;
- The principles of Processing of Personal Data of Employees and candidates,
- The organizational solutions adopted by MC Square
- The procedure of Personal Data Breach management.

MC Square S.A. may collect and use their clients', being the individual or institutional or corporate investors, "hereinafter collectively called the "Clients") and their potential Clients' Personal Data (e.g. name, age and date of birth, address, residence, e-mail etc.) when the Clients or potential Clients are legal entities, MC Square may collect the Personal Data of these companies' representatives, ultimate beneficial owners, authorised signatories etc**.,** for the purposes relating to performance if contracts including pre-contractual arrangements, or to comply with specific regulatory requirements. The Company also collects and uses the Personal Data of its current and former employees for employment related activities exclusively. MC Square may also collect and process the data of its service providers including Personal Data of their employees, officers, directors, beneficial owners etc., for the purpose of the initial and on-going due diligence.

All these natural persons listed below i.e.:

- Clients, potential Clients,
- Client companies' representatives, ultimate beneficial owners, authorised signatories;
- Employees and former employees;
- Representatives, ultimate beneficial owners, authorised signatories, employees of any service providers used by the Company

are the Data Subjects according to GDPR, and MC Square, who determines the purpose and means of the processing, will act as the Data Controller in the meaning of GDPR**.** As the case may be, MC Square may also be processing the Data Subject's data on behalf of another entity e.g. the fund under its managements, in which case latter will be the Data Controller.

1.3.The scope of application

This Policy and the principles herein apply to management (e.g. the members of the Board of Directors, the Conducting Persons, the management and control bodies),and to all employees, including any temporary employees of MC Square (collectively the "Employees").

This Policy set forth guidelines and lay down protection standards that apply to all data Processing by MC Square.

Failure to comply with these guidelines may result in disciplinary action including termination of employment in very serious cases. In addition, these guidelines aim to provide a reference area for activities related to data Processing but exclude all issues relating to logical security, which are dealt with in the Policy "SECURITE DE L'INFORMATION".

The Data Protection Responsible Officer function should be contacted for all issues relating to Data Protection according to the subject being dealt with (see § 2.1).

1.1. Definitions

Breach: an act of breaking or failing to observe a law, agreement, or code of conduct;

Consent of the data: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller:the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Personal data: any information relating to an identified or identifiable natural person ('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;

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor:a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling:any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

2. GENERAL OVERVIEW

2.1. The Organizational approach adopted by the Company

MC Square has adopted the following organizational approach which envisages the division of responsibilities between the Data Protection Responsible Officer and the Conducting Person in charge of IT Department.

Namely:

- Data Security is the responsibility of the IT Department which is under supervision of the Conducting Officer in charge of IT, who defines appropriate guidelines, validates processes and procedures in scope of the first level controls. The second level controls is performed by the Compliance function;
- Data Processing is the responsibility of the Data Protection Responsible Officer who defines appropriate guidelines, validates processes and procedures in scope of the first level controls and consequently designs and executes the second level controls and provides advice/opinions.

MC Square has decided not to appoint a Data Protection Officer " DPO", as they has assessed that given the limited amount of data being processed and the size of the Company, the implementation of this requirement is not necessary. However, the Company decided to appoint the Compliance Officer to acts as Data Protection Responsible Officer (the "DPRO") who will oversee the implementation and application of data protection rules.

2.2. The Organizational approach adopted by the Company

We will keep your information confidential and only use it within MC Square S.A., and only transfer it to third parties in the manner described in the below section labelled "Communication of Personal Data to third parties", unless we are under a duty to disclose or share your personal data in order to comply with a court order or other legal or regulatory requirement.

2.3. General principles of Data Processing

The Company, in the course of its activities, carries out various types of Personal Data Processing that complies with the following general principles:

- Data must be processed fairly, lawfully and in a transparent way;
- Data must be collected for specified, explicit and legitimate purposes and not subsequently processed in a way incompatible with those purposes;
- Data Processing must be adequate, relevant and must not be excessive in relation to the purposes for which data was collected and/or subsequently processed;
- Data must be accurate and, where necessary, updated. Reasonable steps must be taken to ensure that data which is inaccurate or incomplete is erased or rectified;
- Data must be kept in a form which permits identification of Data Subjects and for no longer than is necessary for the purposes for which it was collected or processed and for as long as required by law.

Moreover:

- Data must be processed in a confidential manner and stored in a way and places which ensure appropriate security and restricted access to it;

- Surveillance at workplace shall be possible only to the extent strictly limited by law.

It is the responsibility of the DPRO to ensure that these principles are complied with.

Access to Personal Data must be based on appropriate authorization and a clear need for its use connected with one of the lawful grounds for processing as set out in the GDPR. Every third party receiving the access to Personal Data held by the Company is responsible for protecting it and for being compliant with the applicable data protection laws and regulations. MC Square is responsible for ensuring that such third party is subject to regular monitoring through proper due diligence.

At MC Square any suspected breach of the rules set forth in this Policy must be reported to the DPRO.

3. GENERAL OBLIGATIONS

The Company complies with the following requirements when Processing Personal Data:

- **Information notice to the Data Subject:** The Data Controller must ensure that the Data Subject receives the following information when the Personal Data is obtained directly from the Data Subject. The below information shall be provided at the time when personal data are obtained :
  - The details of the Data Controller and, where appointed, the Data Processor;
  - The purposes, and legal basis for the Processing;
  - Where the Processing is based on the legitimate interest pursued by the Data Controller or by a third part, this legitimate interest shall be communicated;
  - The recipients or categories of recipients to whom data is communicated;
  - The possibility of transfer of the Personal data to third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable means by which to obtain a copy of them or where they have been made available;
  - The voluntary or mandatory nature of providing the requested data as well as the possible consequences of failure to provide data;
  - The existence of the rights listed in section 4 below and how they may be exercised;
  - The period for which the Personal data will be stored, or if that is not possible, the criteria used to determine that period.

MC Square is not obliged to provide the Data Subject with the information which Data Subject already has. Pursuant to accountability rule MC Square shall be able to demonstrate which information the Data Subject has already obtained.

When the data have been obtained from other source than the Data Subject, within a reasonable period after obtaining the data, but no later than one month, the Data Controller must ensure that the Data Subject in addition to the above information receives also information about the categories of data concerned and the source from which the data originate and whether this was a publicly accessible source.

MC Square is not obliged to provide the Data Subject with the information when:

a) The Data Subject already has the information;

b) The provision of such information is impossible or would involve a disproportionate effort;

c) The Data Controller is subject to national or European law requirements which provide appropriate protection for Data Subject's legitimate interests;

d) The data must remain confidential due to professional secrecy obligations binding the Controller.

Other particular obligations of Data Controller:

- **Data Subject's consent**: it is one of the legal bases for the lawful processing of Personal Data. MC Square needs to obtain consent when no other lawful basis applies**.** Under GDPR the consent is defined as "*any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data relating to him or her*". MC Square as Data Controller is responsible for obtaining the consent under the advisement from the DPRO. Data Controller provides a clear privacy notice wherever personal data is collected to ensure that the consent is informed and that the Data Subject is informed of their rights. When the consent was not in writing, the fact that it was collected should be otherwise documented. Whenever the consent is obtained from the Data Subject, the latter shall also be informed about the right to withdraw the consent at any time and how to exercise this right. For written consent the Data Subject shall sign the Consent Form which is the Appendix 1 to this Policy.

- **Processing for direct marketing purposes:** Data Subject shall be informed at the latest at the time of the first communication that he/she has the right to object to processing for direct marketing purposes. The Controller will ensure that this information is presented clearly and separately from other information.

- **Implementation of organizational, technical and security measures:** The Data Controller must implement appropriate technical, organizational and security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, unauthorized disclosure or access. This shall include the users' access management procedure, reporting on information security weaknesses and information security events. The Data Controller will put in place a Personal Data Breach Register which template is attached as Appendix 2 to this Policy.

- **Appointment of Data Processor:** The Data Controller may appoint one or more entities as Data Processors. Data Processors must have experience and skill, be reliability and able to offer sufficient guarantees regarding the technical security measures and organizational measures governing the Processing to be carried out. In this context, the Controller will perform an adequate due diligence before appointment of a new Processor. The Data Controller will also take into account if the potential delegate has in place appropriate technical and organisational measures for the fulfilment the Controller's obligations to respond to requests of the Data Subject's rights laid down in article 4 of this Policy. The Data

Processor may only carry out the Processing accordingly to written instructions given by the Data Controller.

- The Data Controller will put in place and keep up to date a Data Processing Inventory (Appendix 3 to this Policy).

4. RIGHTS OF DATA SUBJECT

Each Data Subject has the right to request the Data Controller:

1. To confirm whether or not his/her data is being processed, and when it is, the right to access to his/her data, and to receive a copy of the personal data held by Controller;

2. If appropriate, a rectification of the personal data that are inaccurate;

3. The erasure of the personal data when the Processing is no longer necessary for the Purposes, or it is no longer lawful, or the data have been unlawfully processed, or when erasure is required by other legal obligations, subject to applicable retention periods;

4. The restriction of Processing of personal data where the accuracy of the personal data is contested, the Processing is unlawful, if the Data Subjects have objected to the Processing and in other cases accordingly to article 18 (1) of GDPR;

Each Data Subject has also the right to:

5. Object to the Processing of personal data (including profiling) on the grounds of a legitimate interest that we as Controller pursue, unless there are legitimate grounds for us to do so (e.g., the establishment, exercise or defence of legal claims);

6. Receive the personal data in structured, commonly used and machine-readable format, or to have this data transmitted directly to another controller where technically feasible (data portability right);

7. Withdraw his/her consent at any time, if consent was the lawful ground for processing;

8. In case of transfer of Personal Data outside EU, obtain information about existence or absence of the justification of the country of destination and adequacy of such jurisdiction published by the

European Commission, and when applicable, a copy of, or access to, the appropriate or suitable safeguards that we have implemented;

Whenever the Data Controller receives the Data Subject's request to exercise any of the above rights, he shall be provided with a document confirming the applicants' identity. After the identity has been confirmed such document should not be retained unless it is required for other purposes (such Anti-Money Laundering, for instance).

One month after the receipt of the request, the Data Controller shall provide the Data Subject with information on actions taken regarding the request, this delay may be extended up to two months for complex and multiple requests. The Data Controller shall inform the applicant about that extension and the reason for it. If after the review of the request the DPRO decides that no action will be taken, he should inform the applicant within one month of receipt of the request of reasons for not taking action and on the possibility of lodging a complaint with CNPD.

In order to exercise the Data Subject's right to access his/her data, the Data Subject shall specify which set of data held by MC Square he/she seeks by filling in the Access Request Form (Appendix 4) The Data Subject may request all data held on them. Such Access Request Form (hereinafter the "ARF") is immediately forwarded to the DPRO who records the date of receiving the ARF and ensures that the requested data is collected. The copy of information shall be provided in the same form as the ARF was submitted, unless it is technically not feasible. The first copy of the data shall be provided for free, however for any further copies MC Square may charge a reasonable administrative fee.

When the data Processing has been restricted MC Square may only store the data in question, and any processing of the restricted data requires the Data Subject consent, unless Processing is necessary for exercise or defence of legal claims, protection of another person's rights or for reasons of important public interest described in article 18 (2) of GDPR. MC Square shall inform the Data Subject before the restriction is lifted and data will be processed again.

Unless prohibited by any applicable law MC Square acting as the Data Controller will inform all recipients about any rectification, erasure or restriction of data which have been disclosed to them.

MC Square shall facilitate the exercise of the above rights, and shall execute them without undue delay.

All requests and complaints regarding Processing shall be sent to email: operations@mcsquare.lu with copy to alecoq@mcsquare.lu and ahecklen@mcsquare.lu

5. DATA PROCESSING

5.1. Communication of Personal Data to third parties

MC Square does not communicate the Personal Data to third parties unless:

- Necessary for the performance of a contract and in an appropriate manner under the applicable data protection regulation;
- There is a provision of law that requires such communication e.g. for purposes relating to anti-money laundering regulations, prevention of fraud, bribery or market abuse, for the regulatory and tax reporting purposes etc.;
- The relevant consent has been obtained from the Data Subject;
- Required by any judgement of court or tribunal and any decision of an administrative authority, however if coming from a jurisdiction outside the EU, such transfer of data may only take place on the basis of mutual legal assistance treaty in force between the requesting country and EU or Luxembourg.

MC Square takes every necessary precaution to ensure the legality and protection of such communication.

Whenever the third party which is either the recipient or the Processor, is located in a jurisdiction outside the EEA, MC Square shall inform the Data Subjects concerned if the country benefit from an adequacy decision, or what kind of safeguards the Data Controller will apply in order to ensure enforceability of Data Subject's rights.

At the time of writing this Policy, the Company does not transfer personal data outside the limits of the European Union. In the event that personal information should be transmitted to a third party outside the country, the Company should then ensure that the destination jurisdiction is recognized as adequate by the European Commission and that the communication channels are sufficiently secure.

5.2. Protection measures

The Company uses appropriate administrative, technical, physical and security measures to:

- Meet the legal requirements and any specific requirements set forth in labour agreements in place with the Employees;
- Safeguard Personal Data against loss, theft and unauthorized access, use or modification;
- Keep Personal Data accurate, complete and up-to-date;
- Ensure that the Processors processing the data apply adequate security and safeguard measures;
- Ensure that the Processors have in place adequate organisational and technical measures which will allow the Controller to comply with the GDPR requirements.

5.3. Retention of Personal Data

Personal Data is generally retained only for as long as is needed to meet the purposes for which it has been collected or as provided for by contract or legal requirements in the country in which the data is **collected and processed or according to document retention requirements.**

MC Square may retain the documents which contain Private Data either in hard copies or/and in electronic copies, which are stored on its secured IT server.

After the required retention period the documents which contain the Private Data will be destroyed.

5.4. Processing of online data

When processing personal information collected during visits to the Company website, MC Square consistently observe the rules laid down in applicable data protection laws. An online Privacy statement is available on the Company website to explain the types of information collected when the public visit the website and outline precisely how the Company uses this information.

6. DATA PROTECTION IMPACT ASSESSMENT

When a processing operation is likely to create a high risk for the rights and freedoms of the individuals concerned, such as for example with the use of a new technology of data processing and/or communication, MC Square shall conduct a Data Protection Impact Assessment ("DPIA").

6.1. Risk Factors

There are nine factors that determine whether a risk criterion is high:

- The evaluation or scoring on the concerned Data Subjects;

- The automated decision making with significant legal effect or similarly effect;

- The systematic supervision;

- The involvement of sensitive data or highly personal data;

- The large-scale data processing;

- The cross-referencing or combination of databases;

- The involvement of data concerning vulnerable persons;

- The innovative use or application of new technological or organizational solutions;

- Where the processing entails a restriction of the rights and freedoms of the persons concerned.

In any case, the DPRO may consider that even if a processing operation meets only one of these criteria, a DPIA is still necessary.

6.2. Objectives of the Assessment

A DPIA is a process whose purpose is to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of individuals related to the processing of their personal data, by evaluating them and determining the measures necessary to address them. The DPIA also aims at ensuring and demonstrating compliance with the rules.

Impact assessments are also tools that help identify and minimize data protection risks of new projects. They must include the design of the processing, the assessment of the impact on the privacy of the persons concerned, and the justification of compliance with the fundamental principles of data protection.

The DPIA should be subject to ongoing review and be regularly re-evaluated. Its renewal is mandatory when the associated risks have changed, taking into account the nature, scope, context and purposes of the processing.

If, after the impact assessment, a high residual risk remains untreated, MC Square has the obligation to consult with the CNPD to obtain prior advice on the proposed treatment and risk management.

6.3. Content of the assessment

The DPIA shall include all of the following elements:

a) Details of the treatment

- Description of the treatment
- Necessity of treatment
- Data concerned
- Persons Concerned
- Purpose
- Hardware and software used
- Distribution channels
- Recipient
- Place of storage
- Duration of storage

b) Assessment of necessity and proportionality

- Measures in favour of proportionality of treatment
- Ensure legitimacy and detail of the purpose

- Ensure data relevance and limitations
- Ensure that the duration of storage is limited.

c) Concrete risk assessment

- As for example: illegitimate access, unwanted modification, disappearance of data
- The list of "high risk" criteria
- The evaluation of each risk: origin, nature, particularity, seriousness, probability, potential impacts on the rights and freedoms of the persons concerned
- The context in which risks arise

(d) The list of remedial measures

Measures in favour of the rights of the concerned Data Subjects:
- Ensuring transparency and information for these persons
- Ensuring the right to access and prior consultation of data
- Ensuring the right of data portability
- Ensuring the right of rectification and the right of deletion
- Ensuring the right to object and limit treatment

e) The list of parties involved
- List the persons involved in the Company and among its third parties

f) The identification of the DPO and the data controller

g) The opinion of the DPO

7. EMPLOYEES DATA AND DATA OBTAINED FOR THE PURPOSE OF RECRUITMENT PROCESS

The Employees are considered as Data Subjects and consequently benefit from the right listed in point 4 of this Policy. In order to exercise their right they should directly contact the DPRO. Data Controller is required to ask the Employees for consent if he plans to process sensitive data like disability, ethnic origin etc.

Candidate's data like name, address, email address, employment history are considered as Personal Data, and the candidates shall be considered as Data Subjects. The Data Controller is entitled on the basis of the legitimate interest to process candidate's data as long as it is job related information and only when the Company intends to contact sourced candidates within 30 days. When sourcing candidates online the Data Controller can only keep a candidate's data without informing them for 30 days, after that time Data Controller must delete their data immediately.

Data Controller is required to ask for consent when process sensitive data like disability, ethnic origin etc. information of the candidate.

The person in charge of recruitment who contacts the candidates shall provide the candidate with a relevant Privacy Notice describing his/her rights or provide the required information by other mean and document it. This information should clearly state that the data will be used for recruitment purposes only and disclose for how long it will be held.

The candidates' Personal Data shall be deleted within one month after obtaining the information if the candidate has never been contacted, or after receiving the candidate's request do erase the data. Documents which contain the Personal Data of candidates obtained before May 26th, 2018, and which are no longer used for a purpose of a recruitment process shall be destroyed.

8. NOTIFICATION OF A PERSONAL DATA BREACH

In the case of a personal data breach, the Company shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to, the competent supervisory authority (the CNPD) , unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. MC Square shall notify the CNPD by using a relevant form published on the supervisory body's website. If the notification is not made within the above time, it shall be accompanied with justification of the delay.

MC Square establishes and maintains an up to date record of all personal data breaches accordingly to Personal Data Breach Register (Appendix 2).

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, MC Square shall communicate the breach to the Data Subject without undue delay by using the Personal Data Breach Notification Form (Appendix 5). Notification to Data Subjects will not be required if:

a) MC Square used appropriate technical and organisational protection measures like encryption, which render the personal data unintelligible to any person;

(b) MC Square has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subject is no longer likely to materialise;

(c) Notification would involve disproportionate effort. In such a case, MC Square shall instead make a public communication or similar measure to effectively inform the concerned Data Subjects.

9. UPDATE OF THIS POLICY

The DPRO is responsible for review and regular update of this Policy for example after implementation of any new regulations or decisions regarding the Personal Data Protection.

10. TRAININGS ON DATA PROTECTION RULES

The DPRO will ensure that appropriate training on the rules regarding Processing of the Personal Data and its Protection is implemented at MC Square.