Internal Privacy Policy
Version: 1.0

Classification: Internal

Ownership and master copy

Department that owns this document:	Data Protection
Document owner:	DPO
Master copy storage location:	

Approval history

S. No	Version	Reviewed by	Approved by	Approver's position	Date approved	Next review date
1	1.0	Privacy Team	BOD	BOD	18-Jun-2021	

Version history

S. No	Version	Updated by	Date	Description of changes
1	0.1a	Privacy team	09-DEC-2020	Initial draft
2	0.1b	Privacy team	28-JAN-2021	Updated based on inputs from MAS
3	0.1c	Privacy team	10-APR-2021	Finalized document from Privacy team
4	1.0	Privacy team	18-Jun-2021	Approved Document

Contents

1. Introduction 4
2. Purpose 4
3. Applicability 4
4. Definitions 4
5. Privacy principles 6
6. Privacy Notice Requirement 7
7. Lawful Grounds for Processing 7
8. Data Retention and Disposal 9
9. Data Quality 10
10. Cross-border Data Transfers 10
11. Third Party Risk Management 11
12. Data subject Rights 11
13. Personal Data Breach Notification 13
14. Security 13
15. Privacy Training and Awareness 14
16. Consequence Management 14
17. Communicate/ Enquire 14
18. Reference Document 14
19. Refresh Schedule 14

1. Introduction

MAS Capital (Private) Limited is a company having its registered office at 199, Kaduwela Road, Battaramulla, Sri Lanka; which is hereinafter referred to as "**We**" or "**Us**" or "**Company**" or "**MAS**".

In accordance with the requirements of the European Union's General Data Protection Regulation ('GDPR'), MAS has created this, **Internal Privacy Policy** [Hereinafter referred to as **"Privacy Policy" or "Policy"**] in order to demonstrate our privacy commitment to our users.

2. Purpose

The purpose of this policy is to describe the process to provide a framework for MAS and its Affiliates (as applicable) to adhere to GDPR and protect the Personal Data they collect through lawful means.

Affiliates shall mean any one or more business entities which, directly or indirectly, are controlling, controlled by, or under common control with MAS. Control shall mean the ownership of 33% or more of the share capital of a company or having management control of a company

3. Applicability

This Policy applies to MAS and all its Affiliates, as well as the directors, officers, employees, agents, consultants, and independent contractors those who handle personal information / sensitive personal information of EU Data Subjects. The Policy covers personal data provided by all vendors, visitors, existing and prospective customers, existing and prospective employees and EU Data Subjects where such data has been collected, used, disclosed, transferred, amended, stored, or otherwise processed by MAS or on its behalf.

4. Definitions

S.No.	Terms	Definition
1	Personal Data	Personal data means 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. Examples of personal data ❖ Name ❖ Identification number ❖ Contact number

		❖ Residential address ❖ Email address, ❖ Internet protocol address ❖ Account data, etc;
2	Sensitive Personal Data/Special Categories of Data	Article 9 of GDPR defines special categories of personal data as any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Examples of sensitive personal data ❖ Health data ❖ Fingerprints ❖ Facial recognition ❖ Retina scanning ❖ Voice recognition ❖ Physical and physiological characteristics, etc;
3	Data Subject	An identified or identifiable natural person. 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 person. Examples: ❖ Customer ❖ End user ❖ Employee ❖ Website visitor ❖ Prospective candidates for employment
4	Data Controller	Under GDPR, a Data Controller is a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body).
5	Data Processor	A "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data controller.

6	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. This includes activities such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Examples: ❖ Processing customer data for shipment
7	Head of IT Governance and Data protection	"Head of IT Governance and Data protection" is an individual assigned as the responsible agent for driving the data privacy and protection program at MAS.
8	Supervisory Authority	Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

5. Privacy principles

MAS is committed to process Personal data in accordance with its responsibilities and obligations as Data Controllers and Data Processors under GDPR. The following points provide a guidance as to how the Company and its affiliates handles and protects the Personal Data of Data subjects:

- Lawful purpose of processing: Personal Data shall be processed by the Company for a specific, clear and lawful purpose.

- Fair and reasonable processing: Processing of Personal Data by the Company or on behalf of it shall be performed —
  - in a fair and reasonable manner and ensure the privacy of the Data Subject; and
  - for the purpose consented to by the Data Subject or which is incidental to or connected with such purpose, and which the Data Subject would reasonably expect that such Personal Data shall be used for, having regard to the purpose, and in the context and circumstances in which the Personal Data was collected.

- Collection Limitation and Data Minimization: Personal Data shall be collected only to the extent that is necessary for the purposes of processing of such Personal Data.

- **Quality of personal data processed:** Necessary steps are adopted to ensure that the Personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

- **Retention of personal data:** The Company shall not retain any Personal Data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the Personal Data at the end of the processing. The Company shall undertake periodic review to determine whether it is necessary to retain the Personal Data in its possession.

- **Accountability:** The Company shall be responsible for complying with the provisions of GDPR in respect of any processing undertaken by it or on its behalf.

6. Privacy Notice Requirement

MAS shall ensure there are procedures in place to maintain transparency with its Data Subjects and provide the following information to the Data Subject in a manner that is clear, concise and easily comprehensible to a reasonable person and in multiple regional languages where necessary and practicable covering the following details:

- The categories of Personal Data generally collected and the manner of such collection;
- The purposes for which Personal Data is generally processed;
- Any categories of Personal Data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
- The existence of and the procedure for exercise of rights of Data Subject and any related contact details for the same;
- The right of Data Subject to file complaint against MAS to the Supervisory Authority ("SA") or to withdraw his consent, and the procedure for such withdrawal, if the Personal Data is intended to be processed on the basis of consent;
- Where applicable, information regarding cross-border transfers of Personal Data that MAS generally carries out;
- The identity and contact details of MAS and the contact details of the Head of IT Governance and Data protection, if applicable;
- The source of Personal Data collection, if the Personal Data is not collected from the Data Subject;
- The individuals or entities including other Data Controllers or Data Processors, with whom such Personal Data may be shared, if applicable;
- The period for which the Personal Data shall be retained or where such period is not known, the criteria for determining such period;
- Any other information as may be specified by the regulations.

MAS shall ensure that the privacy notice is provided at the time of collection, or, if not collected directly from the individual, as soon as reasonably practicable.

7. Lawful Grounds for Processing

MAS shall ensure that it identifies and documents the applicable grounds for processing for each processing activity involving personal and/or Sensitive Personal Data.

A. Processing based on Consent:

MAS shall ensure that consent is duly obtained from the Data Subject in accordance with the provisions of the GDPR in cases where the processing activities conducted by the Company are based on the legal ground of consent. As per the current business processes, MAS may rely on consent as a legal ground for the following functions:

- Human Resources
- Marketing
- Loyalty program
- To Contact customers, when they fill the contact us form in MAS's websites

When the grounds for a processing activity is Consent of data subject, MAS shall ensure that:

a. Valid consent from data subject is correctly obtained and recorded prior to the commencement of processing personal data, especially in case of processing personal data and sensitive personal data of children.
b. Prior consent/permission is obtained from data subject before disclosure of sensitive Personal Data or information by Organisation to any third party.
c. Mechanisms are in place to facilitate withdrawal of consent by the Data Subject for all processing operations based on consent.
d. In case of Processing of Personal Data pertaining to a child, the Company shall, before processing, verify the child's age and obtain the consent of his/her parent or guardian, in such manner as may be specified by regulations.
e. Mechanisms for renewal of consent when Personal Data is processed in a manner that is not incidental to or connected with the original purpose, and which the Data Subject would reasonably not expect in the context and circumstances in which the Personal Data was collected.

B. Processing without Consent:

MAS shall ensure that Processing activities performed without consent as grounds for Processing for any of the following grounds of Processing activities that are applicable for its operations, where consent from the Data Subject cannot be obtained or relied upon:

a. Processing is necessary pursuant to adherence with law or any order of any court or tribunal
b. Processing for prompt action in case of emergencies (e.g. medical emergency involving a threat to life; epidemics, disaster scenario etc.)
c. Processing for purposes related to employment
d. Processing is necessary for other reasonable purposes pursued by MAS which may include activities, such as fraud prevention, information security, mergers and acquisitions, recovering debt and processing publicly available personal data

C. Processing personal data of EU data subjects:

MAS shall ensure that it identifies and documents the appropriate legal basis for processing personal data of EU Data Subjects. GDPR provides six legal basis for processing Personal Data pertaining to EU Data Subjects:

- Consent – The Data Subject has given permission for the organization to process their Personal Data for one or more processing activities. Consent must be freely given, clear, and easy to withdraw, so organizations need to be careful when using consent as their legal basis. For example, the age of automatically checked consent boxes is coming to an end through GDPR.
- Performance of a Contract –The data Processing activity is necessary to enter into or perform a contract with the Data Subject. If the Processing activity does not relate to the terms of the contract, then that data Processing activity needs to be covered by a different legal basis.
- Legitimate Interest –If legitimate interest is used as a legal basis for processing, MAS shall perform a balancing test to determine if the processing activity outweighs any risks to a data subject's rights and freedoms. Examples of legitimate interests pursued by MAS can include certain marketing activities and fraud prevention.
- Vital Interest – A rare processing activity that could be required to save someone's life. This is most commonly seen in emergency medical care situations.
- Legal Requirement – The processing activity is necessary for a legal obligation, such as an information security, employment or consumer transaction law.
- Public Interest – A processing activity that would occur by a government entity or an organization acting on behalf of a government entity.

8. Data Retention and Disposal

MAS shall ensure that personal data processed by its affiliates and departments are stored only for as long as necessary for the specified purposes and in accordance with the consent obtained from data subjects.

- Personal data shall be retained for as long as necessary for identified business purposes
- When the use of personal data is no longer necessary for business purposes, a method shall be in place to ensure that the data is destroyed in a manner sufficient to prevent unauthorized access to that data or is de-identified in a manner sufficient to make the data non-personally identifiable.
- MAS shall have a documented process to communicate changes in retention periods of personal data required by the business to the data subjects who are authorized to request those changes.

Please refer 'Version Control Procedure' and 'Sample emailer for policy changes'

- Personal data shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by MAS or for the benefit of the data subject. Additionally, MAS has the right to retain the personal data in case of any legal and regulatory requirement in accordance with applicable data privacy laws.
- MAS shall perform an internal review on periodic basis to ensure that personal data collected is used, retained and disposed-off.
- The said retention and destruction requirement applies to all SBUs, processes and systems in all countries in which the Company conducts business and has dealings or other business relationships with third parties.
- The said requirements applies to all personal data processed by the Company.
  Examples of documents include:

- Emails
- Hard copy documents
- Soft copy documents
- Video and audio

Please refer 'Data Retention and Disposal Policy' for more details.

9. Data Quality

- MAS shall ensure that personal data is complete and accurate as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete and current.
- Access to source documents and databases is controlled to ensure that records are not altered or destroyed in an unauthorized manner.
- Personal data is protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- Employees will reach out to the Human Resource department to update/correct the personal data which MAS has in its system. However, an email ID needs to be provided to the customers and vendors through which they contact MAS to update/correct their data.
- MAS should validate the completion of such requests on annual basis to ensure accuracy and completeness of personal data

10. Cross-border Data Transfers

MAS shall ensure that appropriate security controls (such as encryption of data at rest and in transit) and adequate mechanisms are in place to ensure transfer of personal data by MAS to a third country is performed in accordance with the provisions of the GDPR.

In case of cross border data transfers of personal data originating in Sri Lanka, MAS shall ensure that:

1. Cross-border transferred outside Sri Lanka

MAS shall ensure that cross-border data transferred outside Sri Lanka for the purpose of processing:

(a) there is a legally binding and enforceable instrument between MAS and the recipient of the data

(b) MAS shall adopt or enter into other instrument that may be determined by the authority.

2. EU data subjects

With respect to personal data pertaining to EU data subjects, MAS to ensure compliance with the requirements of the GDPR in relation to cross-border transfer of data by indulging in the following activities:

- Review of MAS's existing and planned business operations on an annual basis;
- Identify all circumstances in which personal data is transferred to recipients located outside the EEA (European Economic Area); and
- Ensure that, for each such transfer, the organisation has in place a data transfer mechanism that complies with the requirements of the GDPR with respect to having:

i. Transfers subject to Adequacy Decisions taken by the European Commission
ii. Cross-Border Data Transfer between and within various entities of a parent company can be facilitated by Binding Corporate Rules ("BCRs").
iii. Pre-approved model data protection clauses provided by the European Commission may be used for facilitating transfers between controller and controller / controller and processor.
iv. Codes of Conduct approved by Supervisory Authority ("SA") may be used for facilitating cross-border transfer of data.
v. A Cross-Border Data Transfer may take place on the basis of certifications.
vi. Other derogations such as explicit consent, public interest, etc. provided under the GDPR Article 49

11. Third Party Risk Management

MAS shall ensure that disclosure of personal data to third party vendors/service providers/contract staff engaged in processing of personal data on behalf of MAS are performed in accordance with a defined Third Party Risk Management Policy.

The policy shall entail the requirements associated with on-boarding vendors and service providers and managing on-going relationships to determine a third-party's ability to protect MAS's confidential data and information systems as well as to address any applicable regulatory or legal requirements under the GDPR.

Please refer to the 'Risk Assessment Methodology for Third Parties' for more details.

12. Data subject Rights

MAS envisages fulfilling requests received directly from data subjects or on behalf of the data subjects in an expeditious manner and not later than thirty days from the date of receipt of the request/complaint. Individual Rights Policy applies to all Company divisions and affiliates, where requests are received from employees as well as third parties (including customers, vendors), for the personal data stored in paper and electronic format with respect to the Data subject rights.

- MAS shall ensure that adequate mechanisms (such as data subject access request forms, email ID of the Head of IT Governance and Data protection, etc.) are in place to facilitate and address requests received from data subjects within such period and in such manner as may be specified by regulations.
- MAS shall comply with the request and communicate the same to the data subject, within such period as may be specified by regulations.
- Where any request is refused by organisation, it shall provide the data subject the reasons in writing for such refusal and shall inform the data subject regarding the right to file a complaint with the Supervisory Authority against the refusal, within such period and in such manner as may be specified by regulations.

EU Data Subject Rights:

Under the GDPR, the following rights will be available to EU data subjects:

Right to be informed	To provide Data Subjects with details related to the processing of personal data such as the purpose of processing, recipients of personal data, cross border data transfer if any, etc. , in accordance with Article 12, 13 and 14 of General Data Protection Regulation.
Right of rectification	Data subject has the right to obtain rectification of the incorrect or inaccurate personal data being processed by the Company without undue delay.
Right to object	Data Subjects can object to the processing of their data in cases where the Company is relying on the lawful ground of processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or procession for the purposes of the legitimate interests pursued by the controller or by a third party.
Right to restrict processing	Data Subjects will have the right to restrict processing in the following circumstances: • They contest the accuracy of the personal data (the Company will verify the accuracy of the personal data being contested) • The processing is unlawful, but the Data Subject doesn't intend to erase the personal data • The company no longer needs the personal data for the purposes of the processing, but the data subject for the establishment, exercise or defence of legal proceedings requires them. • The data subject has objected to the processing on the lack of legitimate grounds for processing personal data
Right to data portability	Data Subject has the right to receive the personal data concerning themselves in a structured, commonly used and machine-readable format (e.g. CSV[1], XML[2] or JSON[3]) in cases where the Company is processing personal data of the data subject based on consent or on a contract and the processing is carried out by automated means. The data subject's request can extend to requiring the Company to transmit the personal data to another controller.
Right to erasure	The right to erasure of data will apply, unless required for legal obligation, processing for legal claim : • Where their data is no longer necessary for the purpose it was collected, or processed, or if it was unlawfully processed. • Where the data subject has withdrawn their consent

[1] Comma separated values
[2] Extensible Mark-up Language
[3] JavaScript Object Notation

Right to access	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and if processed details about: ✓ Purposes of the processing ✓ Recipients or categories of recipient to whom the Personal data have been or will be disclosed ✓ Period for which the personal data will be stored
Right to object to automated decision-making including profiling	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects the data subject.

Please refer to the below policies and templates for more details

1. *Individual Rights Policy*
2. *Data subject requests form*
3. *Delay in responding to data subject request*
4. *Denial of request template*
5. *Respond to data subject request*

13. Personal Data Breach Notification

MAS shall ensure that any personal data breach, occurring within the organisation or with a third party processor are identified and notified to the Supervisory Authority ("SA)") as soon as possible and within such period as may be specified by regulations and to the data subject where such a breach is likely to cause harm to any data subject with the following necessary details of the breach (at minimum):

(a) Nature of personal data that is the subject matter of the breach;

(b) Number of data subjects affected by the breach;

(c) Possible consequences of the breach; and

(d) Action being taken by the data controller to remedy the breach.

In the absence of any instructions from the SA, in the interim, the response timelines are affixed as 72 hours from the instance of actual knowledge of the data breach. MAS shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in a timely manner and resolutions are documented and communicated to the data subjects.

(Please refer to the 'Breach notification and reporting procedure' for more details.)

14. Security

MAS aims to maintain reasonable physical, administrative and technical safeguards and other measures to ensure a level of security appropriate to the risk associated with its processing activities and the likelihood and severity of the harm that may result from such processing.

Further, MAS shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

An audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year.

15. Privacy Training and Awareness

MAS shall ensure that a privacy awareness and communication program is in place and supported by a monitoring system that confirms all individuals who process personal data on behalf of organization are appropriately trained on their privacy responsibilities, which is enforced as mandatory training.

(Please refer to the 'Privacy Training Policy' for more details.)

16. Consequence Management

All violations of this policy, standard and/or guidelines are subject to disciplinary action. The specific disciplinary action depends upon the nature of the violation and the impact of the violation. Violations will be handled as per the existing HR processes and could range from a verbal reprimand, to termination of employment/contract and/or legal action.

If a department or function is unable to comply with any requirements detailed within this Policy, an exception shall be obtained. Such exceptions shall be documented, indicating the rationale for the exception and the related risks. Exceptions to this policy shall follow the exception process for prior authorization and approval.

17. Communicate/ Enquire

For any queries and/or clarifications, please contact PrivacyOffice@masholdings.com

18. Reference Document

- Version Control Procedure
- Sample emailer for policy changes
- Data Retention and Disposal Policy
- Risk Assessment Methodology for Third Parties
- Third Party Risk Management Policy
- Individual Rights Policy
- Data subject requests form
- Delay in responding to data subject request
- Denial of request template
- Respond to data subject request
- Breach notification and reporting procedure
- Privacy Training Policy

19. Refresh Schedule

This document shall be subject to review and possible revision annually or if there are any changes. The Head of IT Governance and Data Protection will review the policy and forward it to Information Security Steering Committee for approval.