MENON AND MENON LIMITED

Data Privacy Policy

(Release: June.2020 Version: 1.0)

Table of Contents

1. **Data Privacy Policy** 3

1.1 Objective

1.2 Purpose

1.3 Scope

1.4 Responsibilities

1.5 Compliance

1.6 Policy Principles

1.7 Notice to data principal

1.8 Choice and consent

1.09 Data Collection

1.10 Data usage, Retention and Disposal

1.11 Right to access personal information.

1.12 Data share within MML and third parties.

1.13 Storage of personal data.

1.14 Security of personal data.

1.15 Dispute resolution

1.16 Compliance.

2 **Glossary** 12

3 **Annexure**..13

1) Data Privacy Policy

1.1) Objective:

The purpose of the policy is to maintain the privacy of personal data. Menon and Menon limited (Hereafter referred to as "MML") is adopting concepts and requirements of data privacy policy as per Information Technology Act-2000.

1.2) Purpose:

MML is committed to protecting the privacy and security of personal information of employees, contractors, vendors, associates, customers, interested parties and business partners. MML ensure compliance with laws and regulations applicable.

1.3) Scope:

This policy is applicable for all MML employees, contractors, vendors, associate, customers and business partners who may receive personal information, have access to personal information, or who provide information to MML.

All employees of MML must adhere the data privacy policy when they collect or handle a personal information or process or disposal of personal information. This policy supports organizations commitment to protect privacy of personal information.

All external firms and Third partly vendors associated with or for MML and who may have access to personal information, will be expected to read, understand and comply with the policy. No third party is allowed to access personal information held by the MML without entering into non-disclosure agreement.

1.4) Responsibilities:

The owner of data privacy policy will be **data protection officer (Refer Annexure A)**. The data protection officer shall be responsible for maintenance and accuracy of the policy. Any queries regarding implementation of this policy shall be directed to data protection officer.

This policy shall be reviewed and updated by **data protection officer** in 1st Week of January every year. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization's operating environment or on recommendations provided by an auditor.

1.5) Compliance:

Compliance of data privacy policy will be reviewed by **privacy review committee (Refer Annexure A).** In case where non-compliance is identified, the data protection officer shall review the reason for such non-compliance along with a plan for remedies and report them to privacy review Committee. Further action will be taken after review committee recommendations.

Instances of persistent non-compliance by the individuals concerned shall be subject to action and **MML's Model Standing Order.**

1.6) Policy principles:

This policy describes generally acceptable privacy principles for the protection and use of personal information. This policy shall govern the collection, use, share and disposal of personal information. These principles will comply with the law of land. Below points are covered in the policy.

- Notice
- Choice of consents.
- Right of personal data.
- Data collection
- Data usage, Retention and Disposal
- Storage and Security of personal data.
- Share with third party.
- Quality of data
- Monitoring
- Dispute resolution.

1.7) Notice to data principal:

Notice shall be made readily accessible and available to data principal before or at the time of collection of personal information and otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly through online (E-mail footer / Website / Intranet portals / newsletters etc.) and / or offline methods.

All the websites (including MML portal), and any product and service that collect personal information internally shall have privacy notice.

Privacy notice may include but not limited to below points,

- The organizations operating jurisdiction.
- Type of personal information collected, source and collecting person with contact details.
- The purpose of collection.
- Assurance that the personal information will be used only for the purpose identified in the notice.
- Data collection process and how the information is collected; how the information is used including any onward transfer to third parties.
- Retention and disposal process of personal data.
- Process of accessing the personal information.
- Process to update or correct personal information.
- The process of resolution of disagreement.
- Information protection from third party.
- Disclosure process for third party. Restrictions to third parties for misuse of the personal data. The remedial actions in place for any misuse by third party.
- Security measure taken to protect personal information.
- Monitoring and enforcement mechanism.

1.8) Choice of Consent:

Choice refers to the option the data principals are offered regarding the collection and use of their personal information.

Consent refers to their agreement for collection and use of personal information.

- MML shall implement process for the collections and documentation of your consent to the collection, processing and transfer of personal data.
- Data principals shall be informed the choice available to them with respect to the collection, use and disclosure of personal information.
- Consent shall be obtained (In writing or through E-mail) from the data principal before the time of data collection or at the time of data collection or as soon as practical thereafter.
- If personal information is to be used for the purpose not identified in the notice / contract agreements at the time of collection data collection, the new consent will be obtained and documented.

1.9) Data Collection

Personal information may be collected through offline or online portal. Regardless of the collection method, the same privacy protection shall apply for all personal information collected by the MML.

- Personal data refers to data that let MML know the specifies of who you are and which may be used to identify contact or locate you. (Name, age, gender, contact details etc.).
- Data principal shall not be required to provide more personal information than is necessary for the legal provision or service they wish to be obtained
- Data principal shall be asked to provide personal data relevant for the specified scenario or service.
- MML collects personal data from data principal when they connect with the organization for employment or as a supplier/vendor or as a customer.
- If you apply for job or other opportunity through online or offline you will be asked to submit your personal information such as resume, contact details etc. We will use this information to consider you for the job opening. We may also use this information for contacting you regrading other staffing opportunities.

- We may use a third party service provider to assist us with some features. Our service provider will receive personal information on our behalf and will not be permitted to use for other purpose.
- MML shall review and monitor minimum annually information collected, consent obtained and the notice/ contract agreement identifying the purpose.
- We do not collect or share sensitive personal information such as race and ethnicity, religious and sociological beliefs, sex life, political opinion etc.

1.10) Data usage, Retention and Disposal.

- Personal information may only be used for the purpose identified in the notice/ contract agreements and only if the data principal has given consent.
- Personal information shall be retained for as long as necessary for the business purpose identified in the notice / contract agreement at the time of collection or subsequent authorization by the data principal.
- MML use personal data for general business use. This may include following purpose
  - To respond to your request;
  - To provide services to you including customer service issue;
  - To send communication to you about our services / products.
  - To alert you to new features or enhancements to our services/products.
  - To communicate with you about job opportunities.
  - Legal obligation: We may be required to retain your personal information for legal and compliance reason. We may also use personal information to meet our internal and external audit requirements, information security purposes, and as we otherwise believe to be necessary.
  - Under application law of the land.
  - To respond the requests from law enforcement agencies, regulatory agencies, and other public and government authorises.
  - To send business communication such as RFQ, PO or any general business communication.
- When the use of personal information is no longer necessary for business purpose, a method shall be in place to ensure that information is destroyed in a manner sufficient to prevent unauthorized access to that information.

1.11) Right to access personal information.

- Data principal is entitled obtain their own personal information upon a request made in writing. MML shall provide its response within 3 working days after receipt of written request.
- The data principal shall have the right to request MML to correct errors, misleading, outdated, or incomplete personal information.
- Request to access to or rectification of personal information shall be directed, at the data principal's option, to the manger respective department responsible for personal information.
- MML shall provide information to data principal in plain text format.

1.12) Data share within MML and Third party

Data principal shall be informed in the privacy notice / contract agreement, if personal information shall be disclosed to third parties' / partner firms. The personal data will be disclosed only for purpose described in privacy notice or communicated time to time for consent from data principal as obtained.

We do collect or share any sensitive personal information.

- Within MML: All MML departments will made available personal information for the provision of services. All employees and contractors are required to follow our data protection and security policies while handling personal data.
- Personal information may be shared with third parties only for reasons consistent with the purpose identified in the notice / contract agreement or other purpose authorised by law.
- MML shall notify the data principal on online portal or in writing prior to disclosing to the third parties'/ partner firms for purpose for which consent not obtained previously.
- The third parties shall sign a NDA (Non-Disclosure Agreement) with MML before any personal information is disclosed to third party firms.

1.13) Storage of personal data

MML ensures that information collected is processed according to this privacy notice and the requirements of applicable law of the land. MML has servers, system and applications to securely store personal information.

We collaborate with third parties such as cloud hosting services, supplier, and technology support within India. MML take appropriate steps to ensure the personal data is processed, secured and transferred according to the applicable law.

1.14) Security of personal data

MML uses appropriate technologies and procedures to secure data principals personal information. Information technology and security policy are aligned with widely accepted standards and reviewed regularly to protect your data privacy.

- MML provides reasonable technical, physical and operational security procedure to protect personal data from loss, misuse, alternation and unintentional destruction. We periodically review security procedures for personal data security.
- We place appropriate restriction in place to access personal information.
- We implement appropriate security measures and controls including physical monitor.
- Individual becoming aware of any breach of data protection policy shall notify data disciplinary committee **with 3 hours**.

Dispute Resolution

MML shall define and document an incident and **Model Standing Order** which address the privacy related information.

- The incident and **Model Standing Order** may include clear escalation path up to the executive management, legal counsel and the board based on type and/or severity of the privacy incident. It will define a process to register all the incidents/ complaints and queries related to data privacy.

- MML shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in timely manner.

- An escalation process for unresolved complaints and disputes which shall be designed and documented.

1.15.1) Dispute Resolution Process for Employees.

Employees with inquiries or complaints about the processing of their personal information shall first discuss with their reporting manger / department head. If the manger / department head unable resolve the complaint same will be escalate to Grievance officer.

1.15.1) Dispute Resolution Process for other.

Customers / third party with complaints shall contact Grievance committee in writing.

(Contact person Mr. Jawant Kodak, E-Mail jaywant.kodak@menon.in)

1.15) Compliance

Privacy review team shall conduct internal audit annually to ensure compliance with organization privacy policy.

- Any changes in this policy will be communicated through E-Mail / Menon employee Portal / Menon Website with all the employees, stake holders.

2 Glossary

Term	Definition
Data principal or Person	Means the natural person to whom the personal data referred to, (i) an individual, (ii) a Hindu undivided family, (iii) a company, a firm, (v) an association of persons or a body of individuals, whether incorporated or not, (vi) the State, and (vii) every artificial juridical person.
Personal Data	"Personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.
Personal data breach	"Personal data breach" means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;
Third Party	All external parties – Customers, Contractors, Vendors, Auditors etc. - who have access of MML's information assets or information system.
Sensitive Personal Data	"Sensitive Personal Data" means personal data revealing, related to, or constituting, as may be applicable— (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex status; (xi) caste or tribe;

3. Annexure - A

Sr. No.	Designation	Assigned To	Date
1)	Data Privacy Officer	IT Manager	26.06.2020
2)	Data Privacy Review Team	QMS Team Manager	26.06.2020
4)	Grievance Committee	Grievance Committee	26.06.2020