DATA PROTECTION POLICY

MOTHERSON SUMI SYSTEMS LIMITED

Adopted by the Board of Directors on February 13, 2018

Amended by the Board of Directors on August 10, 2021

Regd. Office: Unit 705, C Wing, ONE BKC,G Block, Bandra Kurla Complex, Bandra East, Mumbai- 400051, India
CIN: L34300MH1986PLC284510
Email: investorrelations@motherson.com; Website: www.motherson.com

TABLE OF CONTENTS

1.	Objectives	3
2.	Applicability of the Policy	3
3.	Definitions	3
4.	Application of the law of individual nations	5
5.	Data generation for and collection	5
6.	Sensitive data processing and sharing	5
7.	Transmission of sensitive data	6
8.	Responsibilities and sanctions	6
9.	Data processing	7
10.	Destruction of sensitive data	7
11.	Corporate data protection	8
12.	Communication	8
13.	Amendments	9

DATA PROTECTION POLICY

1. Objectives of the Policy

1.1 The Motherson Group strongly values the need for a transparent and lawful handling of sensitive data (including third party data). In this backdrop, the data protection policy (this "**Policy**"), has been prepared to adopt a consistent and globally valid data protection and data security standard for processing the sensitive data.

1.2 This Policy is based on following broad principles:

a) data must be sourced, generated and utilized in an ethical and lawful manner;

b) data must be fully protected and secured in all circumstances; and

c) adequate processes must be in place to prevent misuse or loss of data or breach of any statutory / contractual obligations.

2. Applicability of the Policy

2.1 This Policy sets out the obligations of all the Motherson Group Companies with regard to data protection in all forms.

2.2 The procedures set out herein must be followed by each of the Motherson Group Company, its employees (temporary or permanent), contractors, agents, consultants, partners or other parties working on behalf of the Motherson Group Company.

3. Definitions

3.1 In addition to the other capitalized terms used hereunder, the following capitalized terms shall have the meanings set forth below:

(a) '**Applicable Law**' means any statute, law, regulation, ordinance, rule, judgment, rule of law, order, decree, ruling, bye-law, approval of any competent authority, directive, guideline, policy, clearance, requirement or other governmental restriction or any similar form of decision of or determination by, or any interpretation or administration having the force of law of any of the foregoing by any competent authority having jurisdiction over the matter in question, whether in effect as of the date of this Policy or at any time thereafter.

(b) '**Data Subject**' means any person who is the owner or provider of Sensitive Data. To be clear, in case of Sensitive Data generated by a relevant Motherson Group Company, the Data Subject for such Sensitive Data will be that Motherson Group Company.

(c) '**Chief Officer**' has the meaning as set out in paragraph 11.2 of this Policy.

(d) '**Concerned Employee**' has the meaning as ascribed to it under paragraph 10.1 (b).

(e) '**Personal Data**' means any information that relates to an identified or identifiable individual.

(f) '**Processing**' means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data.

(g) 'Motherson Group' means the Motherson Group.

(h) 'Motherson Group **Company**' means any company forming part of the Motherson Group.

(i) '**Sensitive Data**' means and includes the following:

(i) Personal Data;

(ii) data/information received from a third party under a non-disclosure agreement/confidentiality agreement;

(iii) data/information regarding the business of any Motherson Group Company or the business of any third party in the possession of any Motherson Group Company;

(iv) communications between Motherson Group Company and its customers, vendors, suppliers, consultants and business partners;

(v) information in connection with any document to which a Motherson Group Company is a party (or is proposed to be a party), whether executed or not;

(vi) any data or information expected to be treated as confidential as per the Applicable Law; and

(vii) any other information in connection with a Motherson Group Company which is reasonably expected to be treated as confidential.

4. Application of the law of individual nations

4.1 This Policy for data protection comprises the internationally accepted principles of data protection, without replacing or overriding the existing national laws. It applies in all cases as far as it is not in conflict with the respective national law; additionally, the national law shall apply if it makes greater demands. National law applies in the case that it entails a mandatory deviation from, or exceeds the scope of, this Policy for data protection.

4.2 This Policy also applies in countries in which there is no corresponding national legislation in place. Each legally independent Motherson Group Company must check whether and to what extent such notification requirements exist. Each Motherson Group Company must obtain annual certification from all its employees for adherence of this Policy.

5. Data Generation and Collection

5.1 Any Sensitive Data must be generated or collected only for a specific purpose and must be adequate, relevant and not excessive with respect to the purposes for which it is generated and collected.

5.2 All Sensitive Data must be protected at all times against unauthorised or unlawful processing, intentional misuse, accidental loss, destruction or damage through appropriate technical and organisational measures.

5.3 In case of Personal Data:

a) The Data Subject must be informed of how individual data is being handled. As a matter of principle, Personal Data must be collected directly from the Data Subject concerned. In processing Personal Data, the individual rights of the Data Subjects must be protected.

b) The records of Personal Data must remain with the human resource department and the human resource department shall be the custodian of Personal Data.

6. Sensitive Data Processing and Sharing

6.1 Sensitive Data may be processed solely for the purpose for which it was obtained or generated. In case, Sensitive Date is to be used for any other purpose, a prior consent from the Data Subject must be obtained before processing the Sensitive Data for such other purpose.

6.2 Sensitive Data may be processed if requested, required, or permitted under the Applicable Law (for any purpose). However, the type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

6.3 For any data (whether or not Sensitive Data) received under any agreement which has confidentiality obligations attached to it, in addition to this Policy, as set out under the respective agreement shall also apply. The recipient of data must ensure that the data is used for the purposes for which it is being obtained and no other purpose. In the event such data is shared by recipient employee with any third party, the recipient employee shall ensure that any such third party to whom data has been disclosed is bound by this Policy and terms of the applicable agreement.

6.4 Employees/representatives of the Motherson Group Companies are forbidden to use Personal Data for private or commercial purposes or to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees/representatives at the start of the employment relationship about the obligation to protect data secrecy.

7. Transmission of Sensitive Data

7.1 For some business processes, it may be necessary to pass on Sensitive Data to third parties. If this does not occur owing to a legal obligation, it must be checked in each instance whether it is in conflict with any interest of the Data Subject that merits protection. When transferring Sensitive Data to a party external to the Motherson Group, the conditions set out in the Policy, must be met.

7.2 Sensitive Data pertaining to the information/data regarding business of a customer of any Motherson Group Company or any other third party must not be sent to a person outside Motherson Group without first obtaining the written consent of such customer/third party.

8. Responsibilities and Sanctions

8.1 The employees of each Motherson Group Company, who bear responsibility for data processing activities of Sensitive Data, are obliged to ensure that legal data protection requirements and requirements formulated in this Policy for data protection are met.

8.2 Management staff are responsible for ensuring that organizational, human resource and technical measures are in place so that any data processing undertaken in their department is carried out in accordance with Applicable Law and with due regard for data protection as per this Policy.

8.3 Each Motherson Group Company and their employees/representatives may only process Sensitive Data in accordance with this Policy. Employees who violate this Policy may be subject to disciplinary action, up to and including dismissal according to policy of respective Motherson Group Company. Employees are expected to report violation of this Policy, and may do so to their immediate supervisor with copies of the violation complaint to the Chief Operating Officer of the respective Motherson Group Company and their respective Head of Regional Chairman Office.

8.4 Any unauthorized collection, processing, or use of Sensitive Data by employees is prohibited. In particular, it is forbidden to use Sensitive Data for personal benefit, to disclose it to unauthorized persons, or make it available in any other way.

9. Data Processing Security

9.1 Appropriate technical and organizational measures must be implemented in order to ensure data security of Sensitive Data. These measures must safeguard Sensitive Data from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. Such measures relate to the security of Sensitive Data, whether processed electronically or in paper form. These technical and organizational measures form part of an integrated information security management plan, and must constantly be revised/updated in accordance with technological developments and organizational changes.

10. Destruction of Sensitive Data

10.1 In the event, any Sensitive Data is required to be deleted or destructed owing to a contractual obligation, such Sensitive Data should be immediately deleted as per the process set out below:

(b) The relevant employee of a Motherson Group Company leading the project in connection with such contract shall be responsible for carrying out the deletion or destruction of such Sensitive Data ("**Concerned Employee**").

(c) The Concerned Employee must ensure that the Sensitive Data is permanently deleted /destroyed in all its existing forms (including physical and electronic forms). To illustrate, all electronic copies of

such Sensitive Data must be permanently deleted from all systems of Motherson Group such that it cannot be retrieved. Likewise, all hard copies of the documents should be shredded or destroyed in such a manner that it cannot be retraced or reconstructed.

(d) The Concerned Employee must seek confirmation that the relevant data/information has been deleted from all employees/representatives of Motherson Group engaged in the relevant transaction/matter and are reasonably expected to be in possession of such Sensitive Data.

10.2 Upon due completion of the process set out in (b) and (c) above, the Concerned Employee shall confirm the deletion/destruction of such Sensitive Data through a certificate and maintain the record of such certificate.

10.3 In the event, any Sensitive Data becomes obsolete, redundant or is required to be deleted, such Sensitive Data should only be deleted after sharing the relevant details of the data with the Chief Information

10.4 Officer/Chief Data Protection Officer, the Group General Counsel and the Head of Taxation of the respective Motherson Group Company and obtaining prior written approval of all three stated above.

11. Corporate Data Protection

11.1 The Motherson Group may from time to time designate internal team or external professional body to supervise the observance of data protection under Applicable Law and/or this Policy.

11.2 The Motherson Group shall appoint a person as the Chief Information Officer/Chief Data Protection Officer ("**Chief Officer**") for Motherson Group who will be responsible for formation of team(s) for observance of data protection as per Applicable Law and this Policy. Until such time, the Chief Officer is appointed or where the office of the Chief Officer becomes vacant, the Chief Operating Officer of MothersonSumi Infotech And Designs Limited shall serve as the Chief Officer.

12. Communication

12.1 This Policy as amended from time to time shall be communicated to all Motherson Group Companies.

13. Amendments

13.1 Any change in the Policy will be subject to review of the Group General Counsel of Motherson Group and adoption by the Board of the relevant Motherson Group Company.

For any clarification / doubt concerning this policy please contact Group General Counsel's Office by sending Email at ***gco_policyquery@motherson.com.*** *Any such email should contain "Motherson Group Data Protection Policy" in the subject line.*