FIEM INDUSTRIES LIMITED

DATA PROTECTION & PRIVACY POLICY (DPP)

1. Introduction and Objective

1.1 Fiem Industries Limited (FIEM/ Company) is a leading manufacturer of automotive products and is among most preferred Tier-1 suppliers to all leading Original Equipment Manufacturers (OEMs) for Automobiles and cater the requirements of OEMs not only in India but also for their international models in global markets. Company also exports its products in many countries. Hence, Company strongly values the need for lawful handling of personal data, sensitive data (including third party data) to maintain its protection and confidentiality. With this background, the Data Protection & Privacy Policy (DPP) has been adopted, so that data security standards for usage, processing and storage of the sensitive data can be adopted as framework.

2. Guiding Principles

2.1 This Policy is based on following broad Principles:

(a) Lawfulness, Fairness, Transparency, Purpose, Minimization and Accuracy:
Data must be sourced, generated and utilized accurately, in an ethical, fair, transparent and lawful manner and only that much as required for the purpose.

(b) Storage:
Data must be fully protected and secured in all circumstances; and

(c) Integrity, Confidentiality and Accountability

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

2.2 The above key principles sets out guidance related to the processing of personal data, which controllers (i.e. those who decide how and why data are processed) need to be aware of and comply with when collecting and otherwise processing personal data.

2.3 These principles should be understood as the fundamental overarching principles which aim to ensure compliance with the spirit of data protection laws and the protection of the rights of individuals.

3. Application of the Law / Regulatory Provisions / Confidentiality Contracts

This Policy comprises the guiding principles and basic provisions for data protection and privacy, which are supplemental and not in derogation or replacement of the existing applicable law in any geography for Data protection and privacy. Further, in case the requirement under any applicable law or confidentiality contracts are more stringent, then the requirement under that applicable law and confidentiality contracts shall prevail.

4. Applicability of the Policy

4.1 This Policy sets out the obligations of the Company with regard to data protection in all forms.

4.2 The provisions set out herein must be followed by Company and its employees who are responsible for data handling, including contractors, agents, consultants, partners or other parties working on behalf of the Company.

5. Definitions

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

(a) '**Applicable Law**' means enacted laws, rules, regulations, directives, ordinance, orders by competent authorities, as in force from time to time in the geography and country, where Company operates and Company is under obligation to comply the Applicable Law with respect to Personal Data.

(b) '**Data Subject**' means any person who is the owner or provider of Sensitive Data. In case of Sensitive Data generated by a company, the Data Subject for such Sensitive Data will be that company.

(c) '**Personal Data**' means any data about any individual who is identifiable by or in relation to such data.

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

(e) **'Sensitive Data**' means the following data:

(i) Personal Data;

(ii) data/information (which is material in its context) and received from a third party under a non-disclosure /confidentiality agreement;

(iii) any data or information (which is material in its context) and expected to be treated as confidential as per the Applicable Laws and Confidentiality or Non-Disclosure Agreements signed with third parties; and

(iv) any other information in connection with Company which is reasonably expected to be treated as confidential.

6. Data Generation and Collection – Responsibility

6.1 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.

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

7. Personal Data – handling Responsibilities:

7.1 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.

7.2 The records of Personal Data must remain with the Human Resource Department and the Human Resource Department shall be the custodian of Personal Data.

8. Sensitive Data Processing and Sharing- Responsibilities:

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

8.2 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.

8.3 For any data (whether or not Sensitive Data) received under any agreement which has confidentiality obligations attached to it, in addition to this Policy, the conditions, as set out under the respective confidentiality 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 no lesser stringent terms of confidentiality than under applicable agreement.

8.4 Employees/representatives of the Company 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.

9. Transmission of Sensitive Data – Responsibilities:

9.1 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 Company, the conditions set out in the Policy must be met including execution of a confidentiality agreement, if not executed earlier.

9.2 Sensitive Data pertaining to the information/data regarding business of a customer of Company or any other third party must not be sent to a person outside Company unless, the recipient is subject to confidentiality obligation under a confidentiality agreement.

10. Data Handling Responsibilities by Person Responsible for the same

10.1 The employees of Company, who are responsible for data processing activities of Sensitive Data, are obliged to ensure that legal data protection requirements and requirements formulated in this Policy are in place.

10.2 Company and its employees / representatives may only process Sensitive Data in accordance with this Policy. Employees who violate this Policy may be subject to disciplinary action, including dismissal / termination of their employment and may also be subject to appropriate legal action and damages according to applicable laws and policy of the Company. Employees are expected to report violation of this Policy, and may do so to their Department Heads with copies of the violation complaint to the Chairman & Managing Director / CFO or Company Secretary.

10.3 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 makeit available in any other way.

11. Data Security Measures – Management Responsibilities

11.1 Management shall ensure 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 principles enumerated under this Policy.

11.2 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 must be revised/updated in accordance with technological developments and organizational changes.

12. Destruction of Sensitive Data – Provisions

12.1 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:

(a) The responsible employee (Designated Employee) of the Company leading the project in connection with such contract shall carry out the deletion or destruction of such Sensitive Data after due approval from any one of CMD, CFO or Company Secretary.

(b) The Designated Employee must ensure that the Sensitive Data is permanently deleted /destroyed in all its existing forms (including physical and electronic forms).

(c) The Designated Employee must carry out the deletion on its own, and certify to any one from CMD, CFO or Company Secretary that the relevant data / information has been deleted permanently from all employees / representatives

of Company engaged in the relevant transaction / matter and who are / were in possession of such Sensitive Data or expected to have such Sensitive Data.

12.2 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 CMD or CFO or Company Secretary and obtaining prior written approval of any of stated above.

13. Corporate Data Protection – Data Protection Officer

13.1 The Company 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.

13.2 The Chairman & Managing Director may designate an officer as the **Data Protection Officer** who will be responsible for observance of data protection as per Applicable Law and this Policy.

14. Interpretation and Amendments to the Policy

14.1 Subsequent amendment in Applicable Law, requiring change in this Policy shall have impact as if Policy stand amended to give effect to that amendment and the Policy shall be revised in due course of time.

14.2 The provisions of this Policy can be amended/ modified in due course and shall be approved by the Board of Directors of the Company from time to time in line with any changes in law, Company's philosophy or otherwise.

14.3 For any clarification concerning this policy please contact Company Secretary.

15. Communication of Policy

This Policy shall be communicated internally and shall also be made available on the Company's website at https://www.fiemindustries.com.

****