

Data Privacy and Personal Information Policy

Obligation to Data Privacy and Personal Information

Contents

1. Fundamental Principles
2. Legal Basis
3. Coverage of Privacy Information under the Policy
 - a. Kinds of Information
 - b. Collection of Information
 - c. Disclosure of Information
4. Transfer of Information
5. Data Security of Information under the Policy

1. Fundamental Principles & Objectives

Volkswagen Group Digital Solutions Private Limited (Formerly known as Volkswagen Group Technology Solutions India Private Limited) (hereinafter referred to as "Digital Solutions (India)") is obliged to safeguard privacy of employees, customers and suppliers' data entrusted to Digital Solutions (India) against improper use. Above and beyond compliance with legislation and other legal binding agreements, the protection and privacy of personal data is one of the fundamental principles which govern the relationship between Digital Solutions (India) and its employees, applicants, customers, suppliers and others.

2. Legal basis

This policy is based on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, along with any other applicable data privacy laws in India. Personal data may be recorded, processed and used if permitted by the Indian Privacy Rules, if the company is legally required to do so, or if the data subject has given their permission. Processing covers collection, storage, transmission and safeguard.

All words and expressions used but not defined in this policy shall have the meanings as assigned to them in the Information Technology Act, 2000 or rules made thereunder, as may be amended from time to time.

3. Coverage of Privacy Information under the Policy

This policy covers sensitive personal data or information of employees, customers and suppliers and entities.

3.1. Kinds of Information

In this Policy, the term **"Personal Information"** means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person by the information available.

In this Policy, the term **"Sensitive Personal Information"** means Personal Information that also consists of information relating to:

- i. Password;
- ii. Financial information such as Bank account or credit card or debit card or other payment instrument details;
- iii. Physical, physiological and mental health condition;
- iv. Sexual orientation;
- v. Medical records and history;
- vi. Biometric information;
- vii. Any detail relating to the above clauses as provided to body corporate for providing service; and
- viii. Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise;

The above information does not cover any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

3.2. Collection of Information

- Consent/approval of the provider of sensitive personal data or information (whether employee, customer or supplier etc.) in writing including fax or email need to be taken for providing sensitive personal data or information as described above of usage before collection of such information by Digital Solutions (India) department. Such consent can be written by the provider providing the information; however such withdrawal shall be in writing.
- The sensitive personal data or information may be collected for a lawful purpose connected with a function or activity of Digital Solutions (India) or any person on its behalf and the collection of the sensitive personal data or information is considered necessary for that purpose.
- The sensitive personal data and information provided to Digital Solutions (India) by the provider can be reviewed and amended to correct any discrepancy or incorrectness. Digital Solutions (India) shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information.

3.3. Disclosure/Processing of Personal and Sensitive Information

- Disclosure of sensitive personal data or information by Digital Solutions (India) to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise.
- Use and processing of personal data may be used for the following purposes information:
Shall be shared, without obtaining prior consent from provider of information,
 - With Government Agencies mandated under the law to obtain information including sensitive personal data
 - Information for the purpose of verification of identity,
 - For prevention and detection of frauds
 - Investigation including cyber incidents
 - Prosecutions
 - Order under the court of law
 - Punishment of offences
 - Any other purposes which is required for business purposes in relation to the employment contract or otherwise under an agreement to fulfil the objective of the agreement

- To process job application and employee benefits
- For attainment of any legal obligations of Digital Solutions (India)

4. Transfer of Information

- Digital Solutions (India) or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the Digital Solutions (India) as provided for under this policy.
- The transfer may be allowed only if it is necessary for the performance of the lawful contract between Digital Solutions (India) or any person on its behalf and provider of information where such person has consented to data transfer.

5. Data Security of Information under the Policy

- Digital Solutions (India) has implemented stringent security policies & procedures and is certified for ISO 27001:2013 standard. In addition to group policies for information insecurity it has also developed local policies as per the requirements of land of law. It has implemented administrative, physical and technical measures for information security controls as per its global security standards.

Data Protection Officer

Any concerns, disputes, discrepancies or grievances' with respect to processing of Personal Information can be referred to the designated Data Privacy and Grievance officer as below:

Name: Dr. Aparna Fulambarkar

DPO: dpo.vwits@volkswagen.co.in

Email ID: aparna.fulambarkar@volkswagen.co.in

Volkswagen Group Digital Solutions Private Limited

Embassy Techzone, 9th Floor, 1.3 Congo Building, Rajiv Gandhi Infotech Park,
Hinjewadi - Phase II, Pune - 411057, Maharashtra, India