WEME Global

Data Governance

We are committed to set ambitious targets and take on our responsibility for data governance acting in accordance with Sarbanes–Oxley Act, Basel I, Basel II, HIPAA, General Data Protection Regulatory (GDPR), CGMP and are guided by ISO/IEC 38500.

01 General Principles

We therefore expect our business partners, employees, and stakeholders

- To act with integrity toward our data management regulations
- To comply with the data protection laws applicable
- To embed this commitment into their business operations and
- To actively reduce risk of exposure to data leakages, data privacy breaches and regulatory fines.

02 Data Management

The key focus areas of data governance include availability, usability, consistency, data integrity, data security and privacy.

Management System	We have established a data management system and processes to ensure effective data management throughout the entire organization.
Definition	We broadly define data as documentation and information received, whether in paper, verbally or digital. Data can be generated, processed, or modified to support business operations, strategic decision making and product improvement activities. All information and data provided by Customers are confidential; labelling is not required but recommended.
KPI	Transparency, traceability, impact measurements, continuous improvement activities, communication of our regulations and policies and infrastructure risk simulations are part of our efforts to keep data accurate and safe.
Responsibility	Accountability and responsibilities toward data governance apply to all our stakeholders. We manage operational, financial and ethical risk of adverse effects of poor data quality and increase consistency and confidence in decision making on all levels based on facts.
Control	WEME acts as per EU GDPR rules for Company Personal Data and Data Regulations to minimize the risk of varying likelihood and severity for the rights and freedoms of natural persons exposure.
Security	This includes technical and organizational measures to ensure a level of security appropriate to that risk. The measures referred to in Article 32(1) of the GDPR shall be taken and continuously improved.

03 Data Privacy

Personal data

We may collect or receive personal information for several purposes connected with our business operations. Appropriate security measures have been taken to eliminate unauthorised access to personal data and limited processing.

We verify whether and what personal data we have saved, digitally track and trace usage, execute revocations and undertake activities to eliminate excessive personal information storage over longer times.

Protection

Information and data is shared on a need-to-know basis only and access restricted based on roles & responsibilities.

Data Protection Impact Assessments shall provide reasonable assistance with any data protection impact and consultations with Supervising Authorities or other competent data privacy authorities support our efforts, which consider to be required by article 35 or 36 of the GDPR or equivalent provisions.

Storage

Data is generally stored if the statutory retention obligations exist or the retention is necessary to meet our statutory tasks, and beyond this if guarantee, warranty, or limitation periods have not yet expired, statutory requirements or legal disputes.

04 Data Quality

Master

Our Master Data Management approach supports operational execution and risk management at all levels of the organization and minimizes the limiting effects of poor data quality.

Organization

Assigned responsibilities keep track of our efforts toward achieving our data quality goals at all levels from Top Management to Field Service and Product Design.

Measure

We measure Data Quality based on availability, usability, consistency, and data integrity, to ensure strategic decision making is based on facts.

Control

Throughout the complete lifecycle of the data, data controls are implemented that support business objectives.

05 Information Architecture

Infrastructure

Suppliers are selected based on their data integrity and security measures to keep data and information safe. After passing our qualifying requirements, suppliers are constantly evaluated by our team of experts through performance measurements.

Accessors of data and information shall consider risks that are presented by processing and modification of such.

Security

Everyone is bound to raise concerns in the unlikely event data and information is subject to threats and not protected to its fullest.

06 Digital Collaboration

Collaboration — We promote digital collaboration and usage of IT software tools to work with customers, suppliers, and employees, or other stakeholders.

Footprint — Application of innovative digital tools ensure our continuous improvement efforts toward corporate results, shareholder value, and our responsibility to reduce carbon footprint.

07 Data Subject Rights

Our commitment to data protection regulations and our organization enables us to exercise Data Subject rights as stated by applicable laws.

Notify — Every Data Subject shall promptly notify WEME if under applicable Data Protection Law in respect to personal data legal requirements are not or partially fulfilled.

08 Report

Report — To resolve gaps, we encourage you to help us resolve the issue by reaching out to WEME or in reference to personal data submit a complaint to the Data Protection Authority.

For more information see **www.wemeglobal.com,** contact WEME Global directly or use **compliance@wemeglobal.com** to get in touch.

09 Effective Date

Pursuant to Management Board decision of WEME Global GmbH on 28th August 2021

This policy extends to the operations and business activities of WEME Global and its affiliates.
In case of conflict between the applicable laws of a country and WEME´s policies, the law becomes precedence. Subject to changes and errors.