



## Data Privacy Policy Principles

Data plays a critical role in the development and operation of manufactured products. How that data is secured, handled, processed, and shared is critical to maintaining consumer and public confidence in the companies that make those products. NEMA advocates for an appropriate balance of an individual's right to their personal data and a manufacturer's duty to provide safe and effective products.

NEMA Members believe in the following data privacy policy principles:

- **Convergence**

Securing data and ensuring consumer privacy in product development cannot be done effectively in a compliance environment which is fragmented by conflicting rules and regulations.

Among the US states, policymakers should seek to enact data privacy statutes that are comprehensive and complimentary to existing local and global statutes. Federally, Congress should establish comprehensive baselines related to data privacy.

- **Due Process**

Data breaches are not created equal: they can result from inadequate system safeguards, human error, a cyberattack, or other event and result in physical, financial, and societal harm. Due process is necessary to ascertain the cause of a breach and recommend an appropriate response. Any investigation or audit by a government agency should be done according to an established set of objective guidelines and certifiable standards which align with the severity of the incident.

- **Innovation**

Many manufactured products require the use of data to ensure their proper handling, security, and maintenance, as well as to function effectively and enhance the user experience. What data is collected and how it is applied relative to the operation of a product varies widely; mandates limiting data inputs could lead to vulnerabilities, compromise system integrity, and slow generational growth and adaptability. The secure and reasonable handling and processing of data should be incentivized and encourage further innovation and product development.

- **Compliance**

A product's functionality relies on the data it receives; to achieve the best outcome it is critical the information a product receives is trusted and secure. Companies should handle consumer information responsibility, protect it from unauthorized access or alteration, and be transparent on its processing and usage. When seeking to craft policies on an individual's right to their data, policymakers should collaborate with the private sector and use objective and clear definitions when constructing those rights.

**Contact:** *Peter Ferrell: Manager, Connectivity and Data Policy: 703-841-3280 | [peter.ferrell@nema.org](mailto:peter.ferrell@nema.org)*

**Updated January 2022.**