Navigate Manufacturing Compliance Landscape with Proactive Approach

Today’s manufacturers face a complex and evolving landscape of cyber security and data privacy regulations. Managed effectively, manufacturing compliance can deliver a competitive advantage in addition to protecting sensitive data from unauthorized access and misuse. However, compliance can prove challenging for companies with limited resources and expertise.

As manufacturing companies navigate the world of Industry 4.0, the amount of data they process grows exponentially. Data collected from customers, suppliers, and partners drives strategy and innovation. But it also presents an attractive target for cyber criminals. Manufacturers have a legal and ethical responsibility to carefully safeguard that data.

Complex Regulatory Landscape

Manufacturers must comply with a host of technical, legal, and corporate regulations as they produce and market products. These regulations aim to protect the rights and interests of consumers while also ensuring fair and transparent data practices.

Since the General Data Protection Regulation (GDPR) came into effect in 2018, the regulatory landscape has exploded. Currently in the United States, twelve states have passed data protection laws such as the California Privacy Rights Act (CPRA).

In addition, PCI DSS imposes standards governing the transfer of credit card data. The Sarbanes-Oxley Act mandates formal data security policies for any publicly traded company. And the Federal Trade Commission (FTC) Act requires companies to demonstrate that they have a plan in place to keep data safe and dispose of it securely.

Further, manufacturers that supply the U.S. government must comply with regulations such as the Defense Federal Acquisition Regulation Supplement (DFARS), governing cyber security. International regulations also come into play when companies conduct business in other countries.

Risk Factors to Consider

While manufacturers that fail to comply with these regulations can incur stiff penalties and reputational harm, several risk factors make compliance challenging. In the first place, to remain competitive, companies have embraced emerging technologies such as machine learning and AI.

These new technologies require massive amounts of data, including sensitive data stored and transferred in the cloud. Many manufacturers do not have a complete picture of the data they collect and the source of that data. They may not fully understand how the data is used and shared or who has access to it. The internet of things (IoT) further complicates the picture.

In addition, the scope of sensitive data has broadened beyond credit card numbers and personally identifiable information (PII). Companies that gather geolocation data, for instance, or data that reveals personal behavior could be violating privacy regulations.

Proactive Approach to Manufacturing Compliance Needed

By adopting a comprehensive and proactive approach to data privacy and protection, manufacturers minimize risk and maximize data value. Several key steps will prove essential to this effort:

- Know what regulations apply – Each year more states enact privacy regulations, and governing bodies regularly modify existing regulations. Consult your legal team or compliance officer to keep abreast of changes.

- Review and update data policies – With an updated view of applicable regulations, review existing data policies to ensure alignment. These policies will govern data retention and access and determine how data can be shared, what data should be encrypted, and so forth. Automate policies where possible to ease enforcement.
- Conduct ongoing compliance monitoring – In addition to regular security and compliance audits, continuous compliance monitoring will alert data stewards to potential compliance issues.
- Leverage AI and machine learning – While AI does introduce some data challenges, it can also form part of the solution. Humans cannot keep up with the massive influx of data to classify and monitor sensitive information. However, automated AI tools can quickly find and tag data using pattern matching and machine learning.

Partner with Data Compliance Experts

The data compliance consultants at Messaging Architects make it their business to stay abreast of the compliance landscape. From data and secure audits to ePolicy consulting and a host of compliance and security services, they have the expertise and tools that manufacturers need.