Understanding Data Sovereignty: Regulations, Security, and Compliance in 2023

What is Data Sovereignty?
Data sovereignty is the concept of control over data, ensuring that the data is owned, managed, and protected by the entity that created it. This concept is particularly important in the context of global regulations and compliance standards.

Data Explosion
By 2026, global data is projected to reach 175 zettabytes (ZB). The exponential growth of data is driving the need for robust data management and security practices.

Why Track, Control, and Secure Data?

- **Data Breaches:** Personal data tops list of most valuable data to replace!
- **Causes Behind Data Breaches:**
  - 83% of data breaches involve email and web attacks.
  - 74% of data breaches take the longer path.
  - 60% of data breaches are caused by human error.

Rise of Data Privacy Laws
In the U.S., there are 13+ states with data privacy laws as of 2023.

Data Sovereignty Challenges

- **75%** of organizations are challenged by cross-border data transfer regulations.
- **96%** are challenged by the need to comply with multiple data sovereignty requirements.

Checklist for Addressing Data Sovereignty: Address Challenges

- **Data Segregation:** Separate data based on sensitivity levels.
- **Data Encryption:** Encrypt data to protect it from unauthorized access.
- **Data Masking:** Mask sensitive data to prevent its use.
- **Data Minimization:** Minimize data collected and stored.
- **Data Retention:** Retain data only as long as necessary.
- **Data Anonymization:** Anonymize data to protect individual identities.

In summary, data sovereignty is crucial for ensuring that data is protected, managed, and controlled by the entity that owns it. With the rise of data breaches and privacy laws, organizations must implement robust strategies to address these challenges.

*Infographic courtesy of Kiteworks.*