

## **Compliance Checklist:**

Company: Botium Toys

Considerations:

1. Geographical Location: Where the company conducts business
2. Payment Processing: How the company receives payments from customers

Compliance Regulations and Standards:

1. The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

- Applicable

Explanation: Although Botium Toys is not directly involved in the energy sector, it is important to consider FERC-NERC compliance if the company relies on critical infrastructure services provided by energy suppliers or partners. Adhering to FERC-NERC regulations ensures the reliability and security of the electrical grid, which indirectly impacts Botium Toys' business operations.

2. General Data Protection Regulation (GDPR)

- Applicable

Explanation: Botium Toys needs to comply with GDPR if it collects and processes personal data of individuals residing in the European Union (EU). Adhering to GDPR regulations ensures the protection of customer privacy and establishes transparent data handling practices. Non-compliance can result in significant fines and damage to the company's reputation.

3. Payment Card Industry Data Security Standard (PCI DSS)

- Applicable

Explanation: As Botium Toys accepts online payments, it must adhere to PCI DSS requirements to ensure the secure handling of credit card data. Compliance with PCI DSS helps protect customer financial information, prevent data breaches, and maintain the trust of customers and payment card providers.

#### 4. The Health Insurance Portability and Accountability Act (HIPAA)

- Not Applicable

Explanation: HIPAA compliance is not applicable to Botium Toys as it primarily focuses on protecting individually identifiable health information in the healthcare industry. Since Botium Toys is not involved in healthcare services or handling health-related data, HIPAA requirements do not apply.