

Compliance Checklist

At Botium Toys, we take the privacy and security of our customers' personal and financial information seriously. Here are the key standards we follow to ensure compliance and protect our customers' data:

- **General Data Protection Regulation (GDPR):** As we expand our services to reach customers in the European Union, we are committed to complying with the GDPR, which ensures the protection of E.U. citizens' data and their right to privacy, both within and outside of the E.U. In the event of a data breach involving E.U. citizens' information, we will promptly inform affected individuals within 72 hours of the incident.
- **Payment Card Industry Data Security Standard (PCI DSS):** We understand the importance of handling credit card information securely and have implemented robust security measures to comply with PCI DSS. This standard requires organizations that store, accept, process, and transmit credit card information to do so in a secure environment. Compliance with PCI DSS is crucial to avoid severe consequences such as monetary fines, forensic audit costs, payment brand restrictions, damage to brand reputation, and potential lawsuit costs in the event of a data breach.
- **System and Organization Controls (SOC) type 1 and SOC type 2:** We follow these standards to evaluate the effectiveness of our internal controls and assess our financial compliance and levels of risk. SOC1 is focused on financial reporting controls, while SOC2 is concerned with information security controls, including customer data safety. By establishing and maintaining appropriate user access for internal and external personnel, we aim to mitigate risk and ensure the safety of our customers' data.

At Botium Toys, we prioritize the protection of our customers' personal and financial information and strive to uphold the highest standards of privacy and security.