

Connecticut

Are mandatory arbitration provisions recognized in your state? If so, are there any limitations to its enforcement?

Mandatory arbitration provisions are recognized in Connecticut and are favorably viewed by Connecticut courts.

What is your state's law, if any, regarding gift cards, subscription services and loyalty programs?

GIFT CARDS:

Connecticut Law prevents an expiration date or inactivity fee on gift cards and certificates. Certain rules and regulations apply to issuance of gift cards and certificates and refund of normal balances.

SUBSCRIPTION SERVICES:

Connecticut Law requires that subscription services such as trial offers or those contracts which automatically renew at the end of the contract term, include various provisions such as notice of cancellation provisions (ex: the right to cancel and the mechanisms for cancellation). Health clubs and other organizations have other more particularized rules and regulations.

What is your state's law, if any, regarding safeguarding consumer credit card or other private data (i.e., cyber security)? / What is your state's law, if any, regarding the collection and handling of financial information?

The Connecticut Data Privacy Act (CTDPA), which took effect on July 1, 2023, requires that entities covered under the law protect personal data in its possession. Covered entities include persons conducting business in the state, or that produce products or services targeted to state residents, and that during the prior year processed the personal data of (1) 100,000 or more customers (not including processing just for payment transactions) or (2) 25,000 or more customers and derived 25% or more of their gross revenue from selling personal data. Under the law, a data controller must establish, implement, and maintain reasonable data security practices needed to protect the personal data in its possession. While CTDPA does not explicitly require a covered entity to use encryption to safeguard personal data, using encryption is generally considered a reasonable data practice when storing and transmitting personal data. State law incentivizes Connecticut businesses (specifically, those that access, maintain, communicate, or process personal or restricted information) to create, maintain, and follow a written cybersecurity program with administrative,

Connecticut

technical, and physical safeguards for the protection of this information that conforms to an industry-recognized cybersecurity framework 2024-R-0049 March 5, 2024 Page 3 of 4 (CGA § 42-901(b)). If they do, the Superior Court is generally prohibited from assessing punitive damages if the business is sued for a data breach. The protection does not apply if the covered entity's failure to implement reasonable cybersecurity controls resulted from gross negligence or willful or wanton conduct. Most current cybersecurity frameworks recommend encrypting all sensitive data when being transmitted or in storage. The Insurance Data Security Law generally requires licensed insurance companies to develop, implement and maintain a comprehensive written information security program based on a set of risk-based criteria (CGA § 38a-38(c)). As part of its plan, a company must determine if protection, by encryption or other appropriate means, of all nonpublic information while it is transmitted or stored is needed to safeguard personal data (CGA § 38a-38(c)(4)(B)(iv)).