Florida Governor Vetoes Cybersecurity Data Breach Immunity Bill: 4 Things Businesses Can Do to Prevent Data Breach Claims

Insights
7.08.24

To the surprise of some, Governor DeSantis recently vetoed a bill that would have provided businesses with a defense to claims arising from "cybersecurity incidents" that lead to data breaches – so long as they met a few critical obligations. According to a June 26 letter from the Governor accompanying his veto, he believed the bill would have resulted in Floridians' data being less secure because it would have provided for "across-the-board protections for only substantially complying with the cybersecurity standards." In light of this development, what are four things Florida companies can do to protect themselves and prevent data breach claims?

Assess Your Data

You can read more about the bill rejected by Governor DeSantis here. Despite the fact that your business might not be able to enjoy the immunity proposed by Florida lawmakers, you still have plenty of incentive to comply with best practices in this field.

According to one study, the global average cost of a data breach in 2023 was $4.45 million per incident. And this is not even accounting for the reputational harm that comes from such incidents. Now more than ever, it is vital for businesses to undertake efforts to reduce the risk and impact of data breaches.

The best way to get started is to take a proactive approach and assess what personal and sensitive data you hold and whether collecting and retaining certain data makes sense for your business. You should also determine whether data should be backed up to the cloud or other devices to ensure business continuity.

- **Require Dual Factor Authentication and Employee Training** – You should require dual factor authentication to access any personal and sensitive data. Additionally, you should provide comprehensive employee training to educate your workforce on security best practices and phishing awareness.
- **Review Contracts with Your Vendors** – Review contracts with your vendors to assess and determine if their security practices meet your requirements.
- **Partner with your IT Department and Strategic Third-Party Providers** – By partnering with your IT department or third-party experts, you can conduct regular security audits and identify

potential liabilities, update software, and assess the need to encrypt sensitive data. Additionally, you should implement intrusion detection and firewalls as necessary.

- **Develop an Incident Response Plan** – You should also assess your business and develop an incident response plan. In the event of a data breach or compromised system, you will want to ensure that you have methods in place for containing any breach and communicating with key stakeholders.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team, the Privacy and Cyber Practice Group, or in one of our Florida offices. We will continue to monitor consumer privacy law developments and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

Ilanit Fischler
Partner
954.847.4723
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Brett P. Owens
Partner
813.769.7512
Email

Service Focus

Privacy and Cyber

Related Offices

Fort Lauderdale

Orlando

Tampa