SpencerFane®

Charting Your Course Through Data Privacy: What Every Business Should Know

Businesses across various sectors are now navigating a complex landscape of data privacy regulations, as the importance of safeguarding personal information continues to gain traction with state legislatures. With an increasing emphasis on privacy rights, several states in the U.S. have introduced or updated data protection laws, signaling a significant shift in how businesses handle consumer data. Already in April this year, two new states have joined the ranks of those with consumer data privacy legislation.

Presently, 16 states have enacted data privacy laws, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia. Additionally, numerous states are in the process of drafting their own legislation. While specific requirements vary from state to state, there is notable overlap in what businesses must do to comply with these regulations. Therefore, it is prudent for businesses to proactively prepare for potential expansion into these markets.

Here's a concise breakdown of what businesses need to consider regarding data privacy:

1. **Comprehensive Privacy Policies:** Every business must have a detailed privacy policy outlining the types of data collected and its intended use. This is now a fundamental requirement for businesses collecting customer information.
2. **Data Processing Agreements:** Businesses acting as data controllers and collaborating with third parties must establish agreements to ensure these parties adhere to the designated data management protocols.

3. **Implementation of Data Security Measures:** It's imperative for businesses to establish robust frameworks to secure the data they collect, ensuring protection against unauthorized access or breaches.
4. **Data Protection Assessments:** Many states mandate businesses to conduct comprehensive assessments related to the personal data they collect. These assessments typically include evaluating project purposes, data processing needs, privacy risks, and mitigation strategies.
5. **Opt-In Consent for Sensitive Data:** In most states, businesses must obtain explicit consent from customers before collecting sensitive data, which varies in definition across states but generally includes information related to race, health, sexual orientation, etc.
6. **Data Minimization:** Nearly all states require businesses to limit the collection and retention of personal data to what's necessary for specific purposes. This ensures that only relevant information is processed and retained for the required duration.
7. **Duty to Avoid Secondary Use:** Data controllers are prohibited from processing personal data for purposes unrelated to the specified objectives without obtaining the consumer's consent.

In light of these evolving regulations, executives and business owners should take proactive steps:

- **Review Current Privacy Policies:** Ensure alignment between existing privacy policies and actual data handling practices.
- **Legal Compliance Check:** Engage legal experts experienced in data privacy law to review privacy policies and ensure compliance with state regulations.
- **Assign Responsibility:** Designate a responsible individual within the company to oversee data privacy compliance and response to consumer requests.
- **Test Response Procedures:** Conduct tests to evaluate the company's ability to respond effectively to consumer requests, ensuring readiness to address privacy concerns.

While many people have waited to see if the U.S. federal government will take action on consumer data privacy that would put an end to the patchwork of individual state laws, no such action is expected to occur at least in the foreseeable future. In the meantime prior to any federal standard, business owners are well-advised to

stay informed and taking proactive measures to comply with data privacy laws. Failure to maintain compliance will increase a business' risk of being sued and/or having governmental regulator scrutiny.

This blog was drafted by Jack Amaral and Jon Farnsworth, technology and privacy attorneys in the Minneapolis, Minnesota office of Spencer Fane. For more information, please visit www.spencerfane.com.