Privacy and Cyber Security Among Top Business Regulatory Issues in 2023

Businesses face a host of challenges this year, from inflation to ongoing concerns with pay equality and supply chain security. These challenges will keep legal teams scrambling to stay abreast of changes in legislation and government regulations. And once again, privacy and cyber security hit the list of top business regulatory issues facing companies of all sizes.

Top Business Regulatory Issues Cover a Wide Range

Business legal teams know to expect common legal concerns such as legislation around worker pay and benefits, discrimination, and intellectual property. And 2023 will bring more of the same. About half of the states will likely raise the minimum wage, for instance. Other states will tackle the pay gap and enact laws mandating paid family leave.

Spurred on by rapid digital transformation and an increasing focus on data privacy, legislation at all levels also highlights the need to protect sensitive information. For decades, companies have had to abide by the standards set forth in HIPAA and PCI DSS, for instance. And in 2018, GDPR came into effect, reflecting widespread consumer concern about personal data.

Now, in the continued absence of a federal privacy law, individual states have begun implementing privacy laws. This results in a complex web of legislation that changes from year to year.

Privacy Law Changes Taking Effect in 2023

The European Union enacted sweeping privacy legislation with the GDPR. In the United States, however, privacy laws have proved much more haphazard. In the wake of GDPR, California led the charge, passing the California Consumer Privacy Act in 2018.

Other states have begun to follow suit. Currently, five states have comprehensive privacy laws, with most going into effect in 2023. Additionally, another fourteen states have introduced comprehensive consumer privacy bills. For businesses that operate across state lines, staying on top of privacy law changes can prove challenging.

Privacy laws taking effect in 2023 include the following:

- California Privacy Rights Act (CRPA) – Effective January 1, this replaces California's original privacy law, granting additional rights to Californians. For instance, it grants consumers the right to limit the collection, use and sharing of their personal data. And it includes increased penalties for mishandling of children's information.
- Virginia Consumer Data Protection Act (VCDPA) – Also effective January 1, the VCDPA gives individuals the right to access and correct their personal data. They can also request that organizations delete their data. And the law requires companies to conduct data protection assessments if they collect personal data for sale or advertising.
- Colorado Privacy Act (CPA) – The CPA takes effect on July 1 and mandates protections similar to the Virginia law.
- Connecticut Data Privacy Act – The CTDPA takes effect on July 1, as well. It guarantees consumers the right to request deletion of their personal data and opt out of having their data

sold or used for targeted advertising. In addition, it requires businesses to post clear privacy notices and implement reasonable data security practices.

- Utah Consumer Privacy Act – The Utah law takes effect at the end of 2023 and will require businesses to give clear notice before processing personal data. It will also require companies to provide an opt out option for consumers.

Focus on Risk Management

The data privacy laws enacted and under discussion, as well as numerous cyber security regulations, underscore the need for businesses to strengthen their data risk management. It will prove important for companies to build defensible programs for achieving regulatory compliance and meeting cyber security needs.

For instance, regulations increasingly emphasize the need for businesses to build clarity around critical data. This means focusing on correct classification of data, allowing organizations to locate and monitor sensitive data wherever it travels.

Other risk management aspects that regulators will consider include timely disclosure of incidents and improved threat and vulnerability management. To mitigate risk, businesses will also need to improve their identity and access management programs. And they will need to manage data retention more effectively and monitor third-party processes around data.

Best Practices for Privacy and Cyber Security

As businesses strengthen their data privacy and security practices, they should build on a foundation of solid information governance. Unless they know what data they have, where it lives and who can access it, they cannot ensure regulatory compliance.

Additionally, regular risk assessments and compliance monitoring will highlight security gaps and areas for improvement. Corporate legal teams should be involved in this process to bring awareness of regulatory changes and promote defensible practices.

To schedule a data security assessment and begin building a comprehensive cyber security and privacy program, contact the data security and compliance experts at eMazzanti Technologies.