New data privacy laws are coming in 2023. Experts say businesses need to be prepared.

https://www.bizjournals.com/bizjournals/news/2022/11/10/data-privacy-laws-business-owners-cpra.html

California and other states will implement new data privacy laws in 2023 that could have implications stretching far beyond their borders. Experts say business owners need to be prepared - particularly for California's sweeping new law. The California Privacy Rights Act takes effect on Jan. 1, 2023, and is expected to reshape the consumer and employee data privacy landscape across the country. The law, passed via ballot initiative in 2022, builds on the California Consumer Privacy Act of 2018 and mandates a series of policies and steps businesses need to take on consumer and employee privacy. That includes allowing consumers access to and the right to delete personal information and prevent the sale of their data. In addition to employers with at least one employee in California, aspects of the law also apply to businesses operating in California that have a gross annual revenue of over $25 million; buy, receive or sell the personal information of 50,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information.

For businesses, compliance with the law could entail investments in technology, as well as numerous changes to processes and internal systems. Per California's law, companies can only use consumer data for state purposes and can only keep that data as long as it states publicly, and prohibits companies from collecting more consumer information than necessary. It also gives consumers the right to correct personal information and limit precise geolocation. California has taken the lead on consumer data privacy in the United States, said Fran Faircloth, partner and member of law firm Ropes & Gray's data, privacy and cybersecurity practice, but other states have followed suit, including Colorado, Connecticut, Utah and Virginia, with many other states contemplating their own laws. That patchwork of laws could cause headaches and confusion, so experts say businesses might want to pick the most stringent of the regulations and form policies around its requirements - while recognizing other states could require their own wrinkles.

"We advise clients where possible to use the high-water mark of whichever law offers the most protection - that is always the safest route," Faircloth said. "It's helpful to have one consistent policy and one consistent treatment of data." She said the CPRA covers company employees as well as business-to-business transactions, which could complicate things for business owners that fall under the legislation. For example, a performance review could be included in the kind of data that could be requested, but a performance review could also include private information about the person reviewing the employee, as well. She said the California law also set up a state-level privacy regulator. Before, privacy issues were handled at the state level by the attorney general, while California will now have a separate, dedicated office. She stressed California's law does not include a private right to action, which means individuals cannot bring suits against companies they feel have violated the new law.

But, for companies that are near the $25 million revenue target, they should start preparing to comply with the law ahead of time. Faircloth stressed that, as more states pass their own laws, it will be important to see if a common language or framework comes out, which could fuel federal-level privacy efforts. She stressed businesses should lean into the intent of these laws, which is to safeguard consumer privacy.

"I think the big principle behind all of this is transparency. And that's a good principle in using people's data generally," Faircloth said. "If businesses go into this with a spirit of trying to be transparent with consumers about things then that will get very far down the road of compliance."

Employers in California will need to let their workers know about their rights to data privacy and give them a mechanism for asking for their data and how they can opt out, said Lyle Solomon, principal attorney at Oak View Law Group, a California-based law firm. But overall it's clear that regulators are becoming more particular and are expanding the applicability of data privacy, Solomon said, especially as companies frequently misuse sensitive data or use opaque means to collect and store data - so-called "dark patterns" that, under the new law, could invalidate the consent the consumer originally gave. "The only way for business owners to navigate through it is by following the law as is. They have to edit their existing privacy policies to reflect the latest changes in the law. They must ensure they do not follow dark patterns and provide their employees with equal data privacy protections. They should also be conscientious while handling 'sensitive' personal data and must have express consent before handling any such data," Solomon said in an email. And, while other states are enacting their own laws, they are following similar principles and fundamentals, Solomon said, which means businesses complying with California's privacy laws are already well on their way to complying with other states. "Given this context, if the business has adequately complied with the Californian privacy

law and the (European Union's General Data Protection Regulation), it will have a good head start to operate and comply with the laws of the other states as they come into force," Solomon said.

Arti Raman, CEO and founder of data protection and ransomware immunity software company Titaniam Cybersecurity, shared some tips on how to stay on the right side of the California law and better protect customers' and employees' privacy in general. They include:

• Getting organized: That means making sure all personal data is identified and managed in known places with proper access control to know where it all goes and who can access it.

• Applying controls: Keep track of who has access to your data and make it available on a need-to-know basis. That means encryption, access control and privileges applied to locations that access personal data. If someone requests modification or deletion of their data, there needs to be a well-defined process for how that will work.

• Anticipating insider or outsider compromise: That means preparing for the possibility of a potential breach or cyber attack by ensuring that personal data cannot be stolen in an unencrypted state. In the event of an incident, it is important to have evidence of your security and privacy controls so that a business can demonstrate that it was not unauthorized access that resulted in the compromise.

But business owners should be locking down consumer data and ensuring its security not just to comply with new laws but for their own good, as well, according to Dimitri Shelest, CEO of technology privacy firm OneRep. "Regulatory uncertainty and the lack of a single compliance standard is obviously costly, though the cost can be difficult to quantify. What's less obvious but more quantifiable is the explosion in crimes against businesses, specifically business email compromise and ransomware," Shelest said in an email.

"These crimes are being fueled by the widespread availability of very detailed, legally collected personal data. If the government won't act, it would behoove businesses to take steps to help employees protect their personal data and, in the process, protect themselves."

According to data from the IC3, the FBI's Internet Crime Complaint Center, business email compromises cost businesses $2.4 billion in 2021, up from $1.8 billion in 2019. BECs dwarf all other types of cybercrime against businesses, and accounted for 34% of 2021

losses from all types of cybercrime. Ransomware schemes cost businesses $49 billion in 2021, up from $9 billion in 2019. But Shelest stressed there are far greater losses in productivity and remediation, and that in an age of remote work, security over data is more important than ever.

"It may be years before we have comprehensive federal legislation to protect data privacy. That is why organizational efforts to prevent cybercrime must include restoring employees' privacy by removing their personal information from the internet. That will make it more difficult for malicious actors to obtain employee data to leverage in their attacks," Shelest said.