BURR FORMAN LLP

United States Privacy Laws – Do You Know If You Are In Compliance?

Articles / Publications
04.12.2022

Is your business one that has not prioritized compliance with data privacy laws because you do not collect personal data about your customers? If so, you are in good company, but it is time to reframe your approach on data privacy. Any organization with employees collects, stores, processes, and likely shares personal information about those employees, even if only to process payroll. All organizations need to carefully consider their obligations to comply with data privacy laws and what it takes to come into compliance. To make those determinations, you need to understand when compliance with consumer data privacy laws is required and what is necessary to be in compliance, including what data is protected, when and how you are allowed to collect that data, how you are required to protect that data, how you may use or share that data, and what options you have to offer the identified individuals with respect to their data.

A lot has been written and discussed about the European Union's General Data Protection Regulation (GDPR) that went into effect, May 25, 2018, and established standards for collecting, storing, processing and sharing personal data collected in the European Union. Compliance with GDPR is a significant undertaking that includes developing and maintaining policies and procedures, implementing and monitoring security measures, and complying with reporting requirements in the event of a data breach, and it can be applicable to companies doing business in the United States under the right circumstances. One of the benefits GDPR provides is a single privacy standard that provides clarity in compliance requirements for organizations collecting, storing, processing, using or sharing personal data, even if the standard

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Intellectual Property

United States Privacy Laws – Do You Know If You Are In Compliance?

sets a high bar.

In contrast, privacy laws in the United States are a patchwork of federal and state laws with differing compliance requirements. Sorting out which laws apply to your business, ensuring compliance with each of those laws, and making sure there are not any conflicting requirements between the laws also is a significant undertaking that requires ongoing attention.

Some of the U.S. Federal Laws that are part of this patchwork of privacy laws include:

- The Health Insurance Portability and Accountability (HIPAA) Act together with Health Information Technology for Economic and Clinical Health (HITECH) Act which provide standards for management of health care information and reporting requirements in the event of a breach.
- The Children's Online Privacy Protection Rule (COPPA) which provides standards for the online collection of personal information from children under the age of 13.
- The Gramm-Leach Bliley Act (GLBA) which applies to financial institutions and companies that offer financial products to consumers and requires them to safeguard sensitive data and to explain their information sharing practices.
- The Payment Card Industry Data Security Standard (PCI DSS) which provides standards for processing payment cards.

Privacy laws enacted by the each of the 50 states and many of the US territories make up the rest of the patchwork of US privacy laws. To further complicate the landscape, there are a variety of different tests for determining if your business has to comply with a particular privacy law. For consumer data protection laws, applicability is usually tied to whether or not one does business in that state or targets goods and services to residents of the state; however, the threshold that constitutes doing business in the state differs by state. Because of this, an assessment of whether or not you need to comply with a given state's consumer protection law must be conducted on a state by state basis, considering the type of information you have about residents of that state as well as the amount of business you do in the state and the amount of data you process in the aggregate.

What is Personally Identifiable Information?
Not only does every state have its own definition of personally identifiable information, but the various federal statutes also have their own definitions which are usually specific to the particular industry or type of data. Any information that meets the definition of personally identifiable information or protected health information can trigger requirements to develop, implement and maintain necessary security measures, notify individuals of any breaches of that security, and offer mechanisms for individuals to exercise their rights in their personal information.

In consumer data protection statutes, the definitions of "personal information" or "personal data" are usually broader than the definitions that trigger breach reporting statutes and include any information identifying, relating to, describing, or reasonably linkable a natural person. The variations by state sometimes exclude information that is already publicly available, information that identifies a household versus an individual, or information held as an employer; however, not all states address those exclusions

United States Privacy Laws – Do You Know If You Are In Compliance?

or address them clearly enough to provide certainty.

Because of the wide variety of definitions for "personal information" or "personal data", businesses that collect, store, use or otherwise receive or process the following types of data should carefully examine their practices:

- name, date of birth, mailing address, email address, phone number, location data, identification number, license plate, customer number,
- financial information, financial account number, credit card or other payment card account number,
- biometric data, race, gender, height, weight, other physical characteristics,
- information held by a doctor or medical facility,
- online identifiers, social media account names, login details, social media posts, photographs, digital images, and video footage (when the individual is identifiable),
- internet protocol (IP) addresses, cookie identifiers, RFID tags, mobile phone advertising identifiers, or
- employment evaluations, customer loyalty histories, and political opinions.

In addition to understanding the data that you collect, process or store, the purposes for which you collect it, how you secure it and with whom you share it, you must also assess whether a particular consumer data privacy law applies to your organization.

Consumer Data Protection Rights

Statutes that provide identified individuals with specific rights related to their personal information are generally consumer data protection laws. Again, GDPR was the first legal requirement of this nature and it expressly enumerates the rights data subjects have with respect to their information, how those rights must be explained to the data subjects, and how those rights must be exercisable. At least some elements of the GDPR requirements are seen in at least some of the state consumer data protection laws in the US, including:

- The right to be informed – about the collection and use of personal data;
- The right to access one's personal data by requesting a copy of the data that is collected, maintained or processed about the individual, and with whom the organization shares the data;
- The right to correct one's personal data if it is inaccurate or incomplete;
- The right to be forgotten or the right to erasure of one's personal data in certain circumstances, with the organization required to honor a legitimate request within thirty days;
- The right to restrict processing or use of one's personal data;
- The right to have one's data provided in a format that can be easily transferred to another electronic system;
- The right to object to how one's information is used for marketing, sales or non-service related purposes, provided they cannot restrict use of their personal data for legal purposes or official business, uses in the interest of the public or use of the data to provide the goods or services they requested

United States Privacy Laws – Do You Know If You Are In Compliance?

from you.

During 2020 over 30 American states and Puerto Rico introduced some type of comprehensive consumer privacy law addressing the rights of identifiable individuals, but so far only four states have passed these laws. Those states are California, Colorado, Virginia and Utah. Nevada has also a privacy law that governs the collection of personally identifiable information through websites, but it is not as broad as the acts of the other four states. The California Consumer Privacy Act has been enforceable since July 1, 2020, but it has been effectively amended by the California Consumer Rights Act that goes into effect on January 1, 2023. The Virginia Consumer Data Protection Act goes into effect on January 1, 2023 and the Colorado Privacy Act goes into effect on July 1, 2023. The Utah Consumer Privacy Act follows with an effective date of December 31, 2023. Each of these states has a slightly different test to determine if your business is subject to the law, but they typically involve consideration of your annual revenue, the amount of business you do in the state, the amount of data you process on a regular basis, and the percentage of your business that relates to the collection and processing of data.

On the surface providing consumers with these rights may seem straight-forward, but in practice developing, implementing and maintaining the right business processes to make sure you meet all of your obligations to the identifiable individuals, in the allowed time frames, can be daunting.

Requirement to Protect
Privacy laws of some states include requirements to implement and maintain appropriate security measures to protect the data in your possession or control. These security requirements vary from general obligations to use "reasonable efforts" to secure the data to very specific requirements regarding the security protocols, including obligations to implement written information security protocols (WISP). Federal privacy laws have similar variations in requirements for security measures.

Although not all states currently have requirements for minimal security efforts that must be employed, that number is increasing. States that have adopted a standard in this area usually follow one of two approaches. One security standard used in many states is the requirement to adopt reasonable security practices based on the nature of the business and the amount and type of data the business maintains and controls. Reasonableness is intentionally a subjective standard, and allows you to account for the nature of your business as well as the nature and quantity of data you control, including how the data is collected; what the identifiable individual is told at the time of collection; the security measures used when the data is at rest and in motion; how and by whom the information is accessed once collected and stored by the organization; if and how the organization modifies the data or processes the data; how, when and with whom the organization shares its data; and how the organization disposes of the data when it is no longer needed.

One of the reasons for a reasonableness standard is that the standard changes as technology changes and better security measures become reasonable. It also allows a single law to apply to all industries and types of information by recognizing that reasonable is different for every organizations. Reasonableness also encourages businesses to take a broad view of security and consider what is reasonable within their organization as well as what others in their industry are doing.

United States Privacy Laws – Do You Know If You Are In Compliance?

Another aspect of these security requirements laws that is important to keep in mind is that in many cases if your organization is required to comply with these laws, you are required to ensure you service providers meet the same requirements.

If you operate in an industry that does not yet have well-articulated privacy standards to use as a guide, there is a lot of publicly available guidance to help you assess whether your position and your security programs are reasonable. The Federal Trade Commission (FTC) acts as an enforcer in the privacy space relying on its authority to stem unfair trade practices. The FTC employs a reasonableness standard to assess a company's data security measures, and has published various guides to explain elements that should be considered for an information security program. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is designed to provide guidance on developing an information security protocol and it provides a risk-based approach to guide development of your protocols while relying on various industry standards and recommendations, as well as guidance from the Center for Internet Security's Critical Security Controls, ISO 27001.

Even under a reasonableness standard, you may find it beneficial to have a written information security protocol (WISP) to provide guidelines and structure for evaluating and adjusting your security protocols as needed. Consistent with the reasonableness requirement, the comprehensive nature of the WISP can be guided by the size of the organization, the nature and scope of its activities; the sensitivity of the information it protects; the cost and availability of applicable tools; the organization’s available resources; and any other factors which drive the organizations ability to create and follow a comprehensive WISP. The WISP can be a useful tool to demonstrate an organization's ongoing commitment to proper security efforts.

Data Disposal

Some state laws also address the requirement to dispose of data when the organization no longer has a business reason to retain it. These data disposal requirements focus on disposing of the data in a manner that does not risk disclosure or compromise of the data through the destruction process. More than 35 states and Puerto Rico already have enacted some type of data disposal requirements. Protecting the data during disposal only makes sense because the effort to protect the data while in use is for naught if the data is picked up by unauthorized actors during the destruction process.

Closing Thoughts

Staying in compliance with data privacy requirements is an ongoing task. New state laws continually are being considered and enacted causing compliance obligations to shift. Maintaining a solid understanding of the data you collect, store, process and ultimately dispose of makes it easier to perform the necessary analysis to stay in compliance when new laws are introduced. Compliance with data privacy requirements goes hand-in-hand with your efforts to secure your systems against cyber-attacks, and both issues should be considered together to establish priorities and develop continuous improvement plans that protect your business operations and the data you control.