CARLTON FIELDS

Compliance Steps for U.S. Privacy and Cybersecurity Laws and Regulations

The particular compliance steps that a business should take with respect to privacy and cybersecurity vary based on the nature of the business, where it does business, its data practices, and how it drafts its business contracts and consumer terms and conditions. There are a number of commonalities in U.S. business today, however, and the below steps could assist a company in complying with many U.S. federal and state privacy regimes, and with preparing for standard contract obligations with other businesses.

- Identify and assess the business's existing privacy governance model, with the most important step being to define the roles and responsibilities for privacy compliance. This would include determining who in the organization will have primary responsibility, authority, and accountability for privacy compliance. For a larger organization, this group would typically include a Chief Privacy Officer (or the equivalent), and others with responsibility for information technology, information security, risk and insurance, marketing and sales, and customer experience.

- Create a data map to determine what information the business collects, how the business uses the information after collection, and where and how long the business stores that information. This step will assist in compliance with laws that require disclosures about data collection and use, and in drafting an accurate privacy policy. Special attention should be paid to sensitive personal information, including Social Security numbers, driver's license numbers, payment card information, and information allowing access to a personal bank account. An entity subject to the Gramm-Leach-Bliley Act should, in particular, review whether it collects and uses the data to provide the agreed financial services, or for some other purpose such as marketing. Understanding that usage will assist the business in drafting any applicable Gramm-Leach-Bliley Act disclosures and in determining whether it qualifies for exemptions from certain state-specific privacy laws. Many larger businesses find that working with an outside consultant, hired through legal counsel, can assist them in running an efficient and productive data mapping project.

- After the data mapping exercise, conduct a legal review of which privacy laws, self-regulatory structures, or contract obligations, apply to the business. From there, the business can create a more accurate task list of privacy compliance steps, which may include revising privacy policies, refreshing contract addenda, and preparing written information security programs. Outside counsel can be of particular assistance at this step, if the business has not already involved them in the data mapping process.

- Review the general privacy policy and associated notices at collection for the business, including any state-specific disclosures or required language. Some businesses may elect to comply with state law through an omnibus privacy policy, and others may wish to separate the obligations into different policies. In addition to a privacy policy, the business may need to create state-specific notices at collection, particularly for those businesses subject to California's privacy laws. Companies that are subject to GLBA should review their GLBA privacy notice and determine whether they will have a standalone notice or incorporate GLBA requirements into a company's larger privacy policy. Finally, a business should determine whether any separate privacy notices are needed for employee data collection and use, or for data that a business collects from individuals in their business capacity only (sometimes known as B2B data).

- Conduct an evaluation of customer, supplier, and service provider contracts as to information sale, retention, and security, with a particular focus on any restriction on use of personal information that is received or sent to a third party. This may require drafting new data processing agreements or adding data processing addenda to existing contracts, to comply with state law. Companies may wish to consult with outside counsel for template addenda that are business friendly or third-party friendly, depending on where the company sits in the relationship and the data's anticipated use.

- If the business processes payments through credit card, either directly or through a third party provider, assess compliance with PCI-DSS or other applicable standards, and any annual certification requirements.

January 2023

- Review and, where needed, create internal policies and procedures for records creation, access, and destruction, and for data security and data recovery. This includes an internal privacy policy.

- Create a data access request system to comply with requests to access or delete specific pieces of personal information or to opt out of the selling or sharing of that personal information, as may be required by state law. Larger businesses, those that sell personal information, or those that otherwise anticipate a high volume of data access requests, may wish to consider using a third-party service provider to organize or automate their response operations.

- If appropriate to the business, create or review the business's written information security program (WISP). This will be familiar to companies that are subject to GLBA's Safeguards Rule or to the New York Department of Financial Services's Cybersecurity Regulation. A WISP is a comprehensive, written plan for safeguarding the personal information of customers. It must include administrative, technical, and physical safeguards that are appropriate to the business's size and complexity, its operations, and the customer information it handles.

- Conduct periodic risk assessments and a security assessment to determine if existing data security measures are aligned with the actual data held by the company, and to identify areas of improvement. Larger businesses often use outside consultants for certain technical testing or program review, and elect to hire the consultant either through the legal department or outside counsel so as to maximize the possibility that the work will be protected by attorney-client privilege.

- Create and test an incident response plan to respond to a data security incident, up to and including a data breach. Review in particular how the business will identify and escalate data security incidents within the company, what the roles and responsibilities of the internal incident response team are, and which outside vendors the business will use. Note that this incident response team will have some overlap with the business's privacy governance structure, but that the skills and relative roles will be quite different.

- Conduct training for management and for employees on the business's obligations under privacy laws and how the business is complying, with an emphasis on how the business is responding to privacy requests under applicable law. This training should include those who will be responding to consumer or other data access requests, and for employees who have a role in privacy governance. If the business has contractual obligations related to privacy, apart from those that the law imposes, consider including a module on those obligations in the training.

- Identify outside experts who will assist with privacy and cybersecurity, including potential forensic reviews, penetration testing, data mapping, administration of data access tools, privacy and cyber insurance providers, and law firms. The business may want to inform those vendors and put in place master services agreements or the equivalent, so that those vendors are on notice to assist in the event of an emergency.

Contacts

John E. Clabby
jclabby@carltonfields.com
www.carltonfields.com/jclabby
813.229.4229

Patricia M. Carreiro
pcarreiro@carltonfields.com
www.carltonfields.com/pcarreiro
305.539.7314

Joseph W. Swanson
jswanson@carltonfields.com
www.carltonfields.com/jswanson
813.229.4335

Eden Marcu
emarcu@carltonfields.com
www.carltonfields.com/emarcu
813.229.4148