CARLTON FIELDS

Bracing for 2023: 10 Steps to Prepare for a New Era in U.S. Privacy

CYBERSECURITY AND PRIVACY | TECHNOLOGY | AUGUST 17, 2021


Joseph W. Swanson


Christina M. Gagnier


Patricia M. Carreiro

On July 7, Colorado joined California and Virginia as the third state to pass comprehensive consumer privacy legislation. All three states have new privacy laws with effective dates in 2023 (though California's Privacy Rights Act has some provisions that took immediate effect). While the laws vary, here are 10 steps companies should take now to ease the transition.

1. Gather your team.

Evaluating, and adjusting to, these new privacy laws, particularly for companies not already complying with the European Union's General Data Protection Regulation (GDPR), is going to require cooperation across many parts of your business. Begin by gathering a team that can help think through issues and solutions and keep their respective teams sensitive to privacy issues going forward.

2. Plan.

Your team will first need an understanding of the laws at play, potential exemptions that may apply to your business, what is required, and when. From there, create a list of what needs to be done by when, and who will do what to make it happen. This involves analyzing the scope of these new laws, your business's practices and goals, how quickly your organization adjusts to change, and your organization's risk tolerance.

3. Build a privacy culture. Start communicating and increasing sensitivity.

These laws will only underscore the importance of privacy professionals keeping their organizations sensitive to privacy issues. Start communicating these new restrictions and danger areas to your team now, especially to your marketing and business development departments that may already have plans for new uses of data. Sensitizing your organization to these privacy issues will take time; if you have not already, start now. Find out what your colleagues want to do, discuss the privacy considerations, and figure out a path forward together, then be ready to adjust. One particularly challenging area for businesses not already complying with the GDPR will be targeted advertising.

4. Create a data map.

Creating a data map facilitates every other element of privacy compliance. If your organization does not already have one, or if that data map needs updating, now is the time. A current and complete data map will help you ensure you are appropriately placing all notices at collection, considering all data processing activities and processors involved, can appropriately respond to data subject requests, and have included requisite provisions in all relevant contracts. Be sure your map captures the full data journey. Know where you keep your data, what data you keep where (particularly if that data might be considered "sensitive"), who can access it, what it is used for, and how long it is kept.

5. Revisit data-related contracts.

Contracts must, among other things, designate responsibility, restrict parties' abilities to use data, require appropriate data safeguards, and provide for cooperation. Contracts can also serve as a valuable tool protecting your organization in case of a data incident. Be sure your contracts appropriately portray your respective obligations and know your contractual rights and obligations, particularly when it comes to a data incident, during which timing can be particularly important. To facilitate this, consider preparing one or several standard data addenda that you can already start incorporating into your new contracts. The more standardized your contracts, the easier it will be to evaluate your obligations.

6. Prepare for data protection impact assessments.

Data protection impact assessments may be new to many U.S. companies, at least in name, but the concept is familiar. Now is the time to familiarize yourself with these assessments and what will be necessary. Templates, such as the one

offered by the U.K.'s Information Commissioner's Office, can be a useful starting point.

7. Solidify your cybersecurity protections.

Safeguarding consumer information remains an important part of any business, particularly given the increasing rate of attacks. Precautions like multifactor authentication, strong password policies, system backups, and rehearsed incident response plans are only a few precautions companies should consider. For more on this point, see our articles on cybersecurity and privacy.

8. Prepare for litigation. Document efforts and consider arbitration and class action waiver provisions.

Even with additional cybersecurity protections and efforts to comply with new privacy requirements, the risk of litigation persists. Indeed, almost half of in-house attorneys surveyed for Carlton Fields' 2021 Class Action Survey predict privacy or cybersecurity suits will be the next big wave in class action litigation. There are, however, steps companies can take to improve their litigation position, including documenting their compliance efforts, avoiding overstating their cybersecurity protections, being forthcoming in their privacy notices, and incorporating terms like arbitration provisions and class action waivers into their agreements.

9. Prepare to process and respect data subject rights.

Companies will need processes to evaluate and handle consumer requests to opt out of sharing (or opt in, in certain instances); limit the use or sharing of sensitive data; know, delete, amend, or port their data within allotted time frames; and sufficient record-keeping to demonstrate their compliance. Companies should also consider whether they have current or planned programs in place that could be considered discriminatory against data subjects who more strongly protect their data.

10. Implement data minimization.

Reevaluate the necessity of the data you collect and how long you keep it. Adjust your intake procedures, paperwork, and document retention policies to avoid collecting or keeping unnecessary data. This will not only prepare you for data minimization requirements but may also lower your costs and potential liability in the event of a cybersecurity incident.