Armstrong Teasdale

January 3, 2023 • Advisory • www.atllp.com

2023 IS HERE, AND SO ARE DATA PRIVACY COMPLIANCE DEADLINES

PEOPLE

Jeffrey Schultz, CIPP/US

F. Scott Galt, CIPP/E

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

The week between the holidays and New Year are notorious for being a relatively slow time in the corporate world. If you were out of the office enjoying time with family and friends at the end of the year, or busy with other year-end tasks, you may have missed three significant data privacy compliance deadlines that occurred between Dec. 27, 2022, and Jan. 1, 2023. Even if you were aware of these deadlines, you may still be navigating how or whether they apply to your business, and whether you need to bolster your level of compliance. These compliance deadlines include the deadline to implement the updated European Standard Contractual Clauses (Dec. 27) and the effective dates of new data privacy legislation in California and Virginia (Jan. 1). The following is an overview of the changes associated with these compliance deadlines, and a preview of other key data privacy dates and deadlines for 2023 and beyond.

EUROPEAN STANDARD CONTRACTUAL CLAUSES – COMPLIANCE DEADLINE DEC. 27, 2022

In June 2021, the European Commission passed significant updates to the Standard Contractual Clauses (the "new SCCs"), creating a module system depending on the relationship of the parties entering into the contract and their data processing roles. Prior to the promulgation of the new SCCs, the EU Commission had an old set of standard contractual clauses (the "old SCCs") that businesses could use to create a lawful basis for a data transfer. The old SCCs were one of the principal ways that U.S. businesses shared and received data from EU-based businesses, following the decision invalidating the former U.S.-EU Privacy Shield in 2020.

In addition to creating different modules, one of the most significant aspects of the decision implementing the new SCCs is that it called for the sunsetting of the old SCCs over a year and a half period. Specifically, the decision required companies to implement and replace the old SCCs with the new SCCs by Dec. 27, 2022, in order to ensure a legal basis for the transfer of data from the EU to the U.S.

For U.S. companies, this means that if you receive data from EU companies or about EU data subjects from a company, you must have had the new SCCs in place as of Dec. 27, 2022. The SCCs are used in a variety of situations, including

where U.S.-based companies with operations around the world share data about EU data subjects with other companies, where U.S. companies have a subsidiary in the EU that shares data with the U.S. company, and where a U.S. company does business with an EU company that shares data with the U.S. company, among other situations. As you can see, the situations requiring use of the SCCs are frequent and numerous for global businesses. If your company collects, receives or processes the data of EU data subjects and you have operations or service providers in the U.S. with whom that data is shared, then your organization should evaluate its data transfer mechanism to determine whether you need to implement the new SCCs.

CALIFORNIA AND VIRGINIA CONSUMER PRIVACY STATUTES – EFFECTIVE JAN. 1, 2023

While California's Consumer Privacy Act (CCPA) has been in effect for three years, the passage of the California Privacy Rights Act (CPRA) which amended the CCPA, ushered in significant changes to the CCPA that took effect Jan. 1, 2023. Among the most significant changes include the extension of the CCPA to employees and job applicants, meaning that companies with California employees and job applicants who meet the thresholds required for CCPA compliance must provide employees and job applicants notice of the company's privacy practices, and afford them rights regarding their personal data. Another significant change to the CCPA that took effect Jan. 1, 2023, is companies no longer are afforded a 30-day cure period for violations of the CCPA. Jan. 1, 2023, also ushers in the era of the right to opt out of data "sharing" under the CCPA, which is defined as sharing data for cross-context behavioral advertising, including among multiple brands of the same parent company. This significant expansion of the CCPA to cover employees, coupled with the lack of statutory right to cure and additional rights afforded to consumers, means that organizations need to ensure they have internal and external practices in place in short order to ensure compliance.

While California often steals the privacy limelight, Virginia's law is a significant development that companies need to keep their eye on. Like the CCPA, Virginia's Consumer Data Protection Act (VCDPA) has certain thresholds a company must meet before it is required to comply, intended to weed out smaller businesses from compliance. Also similar to the CCPA, the VCDPA requires certain notice to consumers of the company's data collection practices, and affords Virginia consumers significant rights regarding their data, including the rights to opt out of targeted advertising, to delete data, and to confirm a company is processing their data and access, update and correct the data being processed. The VCDPA has a 30-day cure period for alleged violations, but companies should still take steps to ensure they are compliant with the new requirements.

Key steps companies should take to prepare for compliance with the CCPA

updates and VCDPA include:

1. Determine whether your organization meets the threshold requirements needed to comply with the CCPA and/or VCDPA.
2. Map your data to understand where it is stored in your systems. This includes customer, client and consumer data, as well as employee, job applicant and HR data.
3. Develop and follow a data retention schedule that applies to consumer, employee and job applicant data that considers how long your organization reasonably needs to maintain data in order to fulfill the purpose for which it was collected.
4. Develop procedures for responding to data subject rights requests, and train parties on how to respond to a request and the various requirements to respond to a request.
5. Update your consumer facing and employee facing privacy notices to account for the new CCPA rights and the VCDPA rights afforded to consumers.
6. Review your vendor management tools, including your data processing agreements and vendor agreements to ensure appropriate language is in place so that the vendor is a "service provider," "contractor" or "processor" to your company.
7. Create technical measures and controls to ensure your organization can comply with Global Privacy Control requirements.

OTHER KEY DEADLINES AND DEVELOPMENTS IN 2023 AND BEYOND

Three additional state consumer privacy laws in Colorado, Utah and Connecticut will take effect in 2023, with Colorado and Connecticut's laws effective July 1, 2023, and Utah's law effective Dec. 31, 2023. While all of these laws are similar in certain ways to the CCPA and/or VCDPA, there are also key differences, which will require companies to prepare early to implement appropriate measures to ensure compliance with all applicable regimes.

In addition to these laws, regulations implementing the CCPA are expected sometime in the first half of 2023. These regulations may provide further guidance on certain aspects of the CCPA, such as consumer's rights regarding automated decision making and the use of algorithms by organizations (which may have particular impacts in the employment space and on employee data), and the Global Privacy Control. Based on guidance from the California Attorney General, businesses are required to honor signals via a Global Privacy Control, including browser settings, plug-ins or other mechanisms sent from the consumer's device, as a method of opting out of the sale or sharing of personal information. Colorado's law contains a similar requirement that companies

must respond to universal opt-out signals sent by consumers as a method of opting out of targeted advertising, sales of data, and the use of their data for profiling. While Colorado's law requires compliance with the universal opt-out in 2024, companies may need to implement significant changes to their websites and technical infrastructure to properly comply with this requirement, and may be in a better place to ensure compliance if they begin these projects early in 2023.

Finally, U.S. and EU privacy stakeholders speculate that 2023 may be the year the EU and U.S. reach an agreement for a new transatlantic EU-U.S. Data Privacy Framework (EU-U.S. DPF) to transfer data of EU data subjects more easily to U.S. organizations, similar to the former Privacy Shield. Companies that are looking rely on the EU-U.S. DPF framework to transfer data, if it is passed, rather than another method such as the SCCs, will likely need to evaluate and undertake additional compliance measures to ensure compliance with the standards set forth in the EU-U.S. DPF.

While compliance with these new requirements and privacy regimes in the U.S. and EU may seem overwhelming, our attorneys can assist with crafting and formulating guidance specific to your company's size, operations and processes to determine whether and how you can best comply with global data privacy requirements. For more information specific to your business needs, please contact one of the authors listed below or your regular AT lawyer.