The Uniform Personal Data Protection Act Is Here

FG Law Blog

July 28, 2021

Krishna A. Jani, CIPP/US

In July 2021, the Uniform Law Commission ("ULC") voted to approve the Uniform Personal Data Protection Act ("UPDPA"). The UPDPA is a model data privacy bill designed to provide a template for states to introduce to their own legislatures, and ultimately, adopt as binding law.

The UPDPA

The UPDPA would govern how business entities collect, control, and process the personal and sensitive personal data of individuals. This model bill has been in the works since 2019 and includes the input of advisors, observers, the Future of Privacy Forum, and other stakeholders. This is significant because the ULC has set forth other model laws, such as the Uniform Commercial Code, which have largely been adopted across the states.

Interestingly, the model bill is much narrower than some of the recent state privacy laws that have been passed, such as the California Privacy Rights Act and Virginia's Consumer Data Protection Act. Namely, the model bill would provide individuals with fewer, and more limited, rights including the right to copy and correct personal data. The bill does not include the right of individuals to delete their data or the right to request the transmission of their personal data to another entity. The bill also does not provide for a private cause of action under the UPDPA itself, but would not affect a given state's preexisting consumer protection law if that law authorizes a private right of action. If passed, the law would, consequently, be enforced by a state's Attorney General.

Applicability

The UPDPA would apply to the activities of a controller or processor that conducts business in the state or produces products or provides services purposefully directed to residents of this state and:

(1) during a calendar year maintains personal data about more than [50,000] data subjects who are residents of this state, excluding data subjects whose data is collected or maintained solely to complete a payment transaction;

(2) earns more than [50] percent of its gross annual revenue during a calendar year from maintaining personal data from data subjects as a controller or processor;

(3) is a processor acting on behalf of a controller the processor knows or has reason to know satisfies paragraph (1) or (2); or

(4) maintains personal data, unless it processes the personal data solely using compatible data practices.

The UPDPA defines "personal data" as a record that identifies or describes a data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data. The bill also defines "sensitive data" as a category of data separate and apart from mere "personal data." "Sensitive data" includes such information as geolocation in real time, diagnosis or treatment for a disease or health condition, and genetic sequencing information, among other categories of data.

The law would not apply to state agencies or political subdivisions of the state, or to publicly available information. There are other carve-outs, as well.

Notably, the model bill also contains several different levels of "data practices," broken down into three subcategories: (1) a compatible data practice; (2) an incompatible data practice; and (3) a prohibited data practice. Each subcategory of data practice comes with a specific mandate about the level of consent required—or not required—to process certain data. For example, a controller or processor may engage in a compatible data practice without the data subject's consent with the expectation that a compatible data practice is consistent with the "ordinary expectations of data subjects or is likely to benefit data subjects substantially." Section 7 of the model bill goes on to list a series of factors that apply to determine whether processing is a compatible data practice, and consists of such considerations as the data subject's relationship to the controller and the extent to which the practice advances the economic, health, or other interests of the data subject. An incompatible data practice, by contrast, allows data subjects to withhold consent to the practice (an "opt-out" right) for personal data and cannot be used to process sensitive data without affirmative express consent in a signed record for each practice (an "opt-in" right). Lastly, a prohibited data practice is one in which a controller may not engage. Data practices that are likely to subject the data subject to specific and significant financial, physical, or reputational harm, for instance, are considered "prohibited data practices."

The model bill has built in a balancing test meant to gauge the amount of benefit or harm conferred upon a data subject by a controller's given data practice, and then limits that practice accordingly.

What's Next

After final amendments, the UPDPA will be ready to be introduced to state legislatures by January 2022. This means that versions of this bill can, and likely will be, adopted by several states over the next couple of years—and perhaps, eventually, lead to some degree of uniformity among the states' privacy laws.

Krishna A. Jani, *CIPP/US, is a member of Flaster Greenberg's Litigation Department focusing her practice on complex commercial litigation. She is also a member of the firm's cybersecurity and data privacy law practice groups. She can be reached at 215.279.9907 or krishna.jani@flastergreenberg.com.*