Uniform Law Commission
NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS

111 N. Wabash Ave.
Suite 1010
Chicago, IL 60602
(312) 450-6600 tel
(312) 450-6601 fax
www.uniformlaws.org

THE UNIFORM PERSONAL DATA PROTECTION ACT (2021)

- A Summary -

The Uniform Personal Data Protection Act, promulgated by the Uniform Law Commission in 2021, applies fair information practices to the collection and use of personal data from consumers by business enterprises. The act applies broadly to any entity that collects or maintains personal data but avoids the high compliance costs for businesses and the substantial enforcement costs for states associated with regulatory regimes modeled after the California Consumer Privacy Act and the European General Data Privacy Regulation. And the act exempts small businesses unless they use personal data in a manner that a consumer would not expect. The act also avoids the First Amendment concerns that arise from privacy laws that greatly restrict information without sufficient justification. By adapting a risk-based approach to privacy regulation, the act protects all data subjects from harmful processing and also offers the flexibility for startups and established firms to innovate.

The Act has several elements that make it more practical, more flexible, and less costly than other models of state privacy legislation. Specifically, the Uniform Personal Data Protection Act does the following:

- Authorizes some data practices, called "compatible data practices", that may be performed without consent. Data processing is a "compatible data practice" if reasonable consumers would expect it to occur, or if the consumer directly benefits from the practice.
- Prohibits data practices that may cause a substantial risk of harm to data subjects, including processing likely to cause embarrassment, harassment, or financial harm and data storage that fails to provide reasonable data security.
- Permits "incompatible data practices"—that is, processing that is neither "compatible" nor prohibited—to be performed, but only with notice and consent.
- Promotes transparency and accountability by requiring companies to post a privacy policy identifying their uses of personal data and by giving data subjects the right to access and correct their data.
- Avoids the substantial First Amendment conflict associated with the right to data deletion.
- Authorizes personal data to be used for tailored messaging (including advertising) as a compatible use. (This provision does not cover the use of personal data to make tailored decisions about the terms of an offer to, agreement with, or treatment of an individual.)

- Requires businesses to engage in a privacy and security self-assessment, and encourages honest self-reflection by shielding the content of the self-assessment from disclosure in subsequent litigation.
- Allows businesses to avoid the costs of multiple compliance protocols by recognizing compliance with similar, or more restrictive, laws from other jurisdictions as compliance with this act.
- Limits the scope of the act to companies that collect non-public data maintained in a system of records designed for individualized treatment of or communication with data subjects, thus avoiding applicability to unstructured forms of information such as email communications.
- Exempts data processing that is already regulated by major federal privacy regimes.
- Encourages the development of voluntary consensus standards by which data controllers, processors, data subjects and other interested stakeholders can engage together to develop standards tailored to the context of particular industries.
- Incorporates enforcement provisions of existing state Consumer Protection Acts that authorize state attorneys general to monitor personal data practices and to seek redress for violations of the act.
- Encourages uniformity of enforcement in the enacting states by authorizing state attorneys general directly or through the National Association of Attorneys General, to coordinate their regulatory and enforcement policies.
- Encourages states to determine for themselves whether a private right of action should be authorized for violation of the act and provides bracketed language to prohibit such rights of action.

The Act uses subtle incentives to encourage more responsible data use. Small businesses are exempt as long as they use only "compatible" data practices. Use of personal data that is pseudonymized (data with personal identifiers removed) is subject to fewer restrictions than data with personal identifiers, thus encouraging entities to convert identified data into a form that offers more privacy and security. The act also authorizes companies to use or disclose data for general research purposes and prohibits the re-identification of pseudonymized or de-identified data. Moreover, in order to avoid unintended increased risk to data subject privacy, the act requires only those controllers who have directly collected data from consumers and who are best position to authenticate their identify, to respond to access and correction requests. All other downstream recipients of personal data must respond to requests that are transmitted by the collecting controller.

For more information about the Uniform Personal Data Protection Act, please contact ULC Legislative Counsel Libby Snyder at (312) 450-6619 or lsnyder@uniformlaws.org.