Uniform Personal Data Protection Act

Amendments

July 10, 2021

* * *

Section 2. Definitions

* * *

(4) "Data subject" means ~~a resident of this state~~ an individual who is identified or described by personal data.

(17) "Sensitive data" means personal data that reveals:

* * *

(D) a Social Security number, tax-identification number, driver's license number, military identification number, or an identifying number on a governmen~~tal~~-issued identification;

* * *

(G) income;

(~~G~~ H) diagnosis or treatment for a disease or health condition;

(~~H~~ I) genetic sequencing information; or

(~~I~~ J) information about a data subject the controller knows or has reason to know is under 13 years of age.

* * *

Section 3. Scope

(a) This [act] applies to the activities of a controller or processor that conducts business in this 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 ~~during a calendar year~~ 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.

(b) This [act] does not apply to an agency or instrumentality of this state or a political subdivision of this state.

(c) This [act] does not apply to personal data that is:

(1) publicly available information;

(2) processed or maintained solely as part of human-subjects research conducted in compliance with legal requirements for the protection of human subjects;

(3) processed or disclosed as required or permitted by a warrant, subpoena, or court order or rule, or otherwise as specifically required by law;

(4) subject to a public-disclosure requirement under [cite to state public records act]; or

(5) processed or maintained in the course of a data subject's employment or application for employment.

* * *

Section 5. Right to Copy and Correct Personal Data

(a) Unless personal data is pseudonymized and not maintained with sensitive data, the collecting controller, with respect to personal data initially collected by the controller and maintained by the controller or a third-party controller or processor, shall:

* * *

(5) make an amendment or correction requested by a data subject if the controller has no reason to believe the request is inaccurate, unreasonable, or excessive; and

* * *

Section 7. Compatible Data Practice

* * *

(b) A compatible data practice includes processing that:

* * *

(6) permits analysis for generalized research or for the research and development of a ~~new~~ product or service. For purposes of this subsection, "generalized research" means the use of personal data to discover insights related to public health, public policy, or other matters of general public interest and does not include use of personal data to make a prediction or determination about a particular data subject. ~~that may provide a public benefit;~~

* * *

Section 8. Incompatible Data Practice

(a) A controller or processor engages in an incompatible data practice if the processing:

(1) ~~the processing~~ is not a compatible data practice under Section 7 and is not a prohibited data practice under Section 9; or

* * *

Section 10. Data Privacy and Security Risk Assessment

* * *

(b) A controller or processor shall update ~~The~~ the data privacy and security risk assessment ~~must be updated~~ if there is a change in the risk environment or in a data practice that may materially affect the privacy or security of the personal data.

* * *

Section 11. Compliance with Other Law Protecting Personal Data

* * *

(b) A controller or processor complies with this [act] with regard to processing that is subject to the following acts or amendments thereto:

* * *

(2) the Fair Credit Reporting Act, 15 U.S.C. Section 1681 et seq. or otherwise is used to generate a consumer report by a consumer reporting agency as defined in Section 603(f) of the Fair Credit Reporting Act, 15 U.S.C. Section 1681a(f), a furnisher of the information, or a person procuring or using a consumer report;

* * *

Section 15. Recognition of Voluntary Consensus Standard

* * *

(c) The [Attorney General] shall determine whether to grant or deny the request and provide the reason for a grant or denial. In making the determination, the [Attorney General] shall consider the need to promote predictability and uniformity among the states and give appropriate deference to a voluntary consensus standard developed consistent with this [act] and recognized by a privacy-enforcement agency in another state.

* * *

Section 16. Applicability of [Consumer Protection Act]

* * *

(c) In adopting rules under this section, the [Attorney General] shall consider the need to promote predictability for data subjects, controllers, and processors, ~~and regulated entities~~ and uniformity among the states consistent with this [act]. The [Attorney General] may:

* * *

[(e) Nothwithstanding subsection (a), a private cause of action is not authorized for a violation of this Act or under the consumer protection statute for violations of this act.]

Legislative Note: *Include subsection (d~~e~~) only if the state's applicable consumer protection act does not provide for the recovery of costs and attorney's fees. Bracketed subsection (e) is only relevant for states that have a Consumer Protection Act that authorizes a private cause of action and it is determined that such a cause of action should not be authorized.*