Uniform Personal Data Protection Act*

Drafted by the

Uniform Law Commission

and by it

Approved and Recommended for Enactment
in All the States

at its

Meeting in Its One-Hundred-and-Thirtieth Year
Madison, Wisconsin
July 9 – 15, 2021

Without Prefatory Note and Comments

July 11, 2021

**The following text is subject to revision by the Committee on Style of the National Conference of Commissioners on Uniform State Laws.*

Uniform Personal Data Protection Act

Section 1. Title

This [act] may be cited as the Uniform Personal Data Protection Act.

Section 2. Definitions

In this [act]:

(1) "Collecting controller" means a controller that collects personal data directly from a data subject.

(2) "Compatible data practice" means processing consistent with Section 7.

(3) "Controller" means a person that, alone or with others, determines the purpose and means of processing.

(4) "Data subject" means an individual who is identified or described by personal data.

(5) "Deidentified data" means personal data that is modified to remove all direct identifiers and to reasonably ensure that the record cannot be linked to an identified data subject by a person that does not have personal knowledge or special access to the data subject's information.

(6) "Direct identifier" means information that is commonly used to identify a data subject, including name, physical address, email address, recognizable photograph, telephone number, and Social Security number.

(7) "Incompatible data practice" means processing that may be performed lawfully under Section 8.

(8) "Maintains", with respect to personal data, means to retain, hold, store, or preserve personal data as a system of records used to retrieve records about individual data

subjects for the purpose of individualized communication or decisional treatment.

(9) “Person” means an individual, estate, business or nonprofit entity, or other legal entity. The term does not include a public corporation or government or governmental subdivision, agency, or instrumentality.

(10) “Personal data” means a record that identifies or describes a data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data.

(11) “Processing” means performing or directing performance of an operation on personal data, including collection, transmission, use, disclosure, analysis, prediction, and modification of the personal data, whether or not by automated means. “Process” has a corresponding meaning.

(12) “Processor” means a person that processes personal data on behalf of a controller.

(13) “Prohibited data practice” means processing prohibited by Section 9.

(14) “Pseudonymized data” means personal data without a direct identifier that can be reasonably linked to a data subject’s identity or is maintained to allow individualized communication with, or treatment of, the data subject. The term includes a record without a direct identifier if the record contains an internet protocol address, a browser, software, or hardware identification code, a persistent unique code, or other data related to a particular device. The term does not include deidentified data.

(15) “Publicly available information” means information:

(A) lawfully made available from a federal, state, or local government record;

(B) available to the general public in widely distributed media, including:

(i) a publicly accessible website;

(ii) a website or other forum with restricted access if the information is available to a broad audience;

(iii) a telephone book or online directory;

(iv) a television, Internet, or radio program; and

(v) news media;

(C) observable from a publicly accessible location; or

(D) that a person reasonably believes is lawfully made available to the general public if:

(i) the information is of a type generally available to the public; and

(ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed.

(16) "Record" means information:

(A) inscribed on a tangible medium; or

(B) stored in an electronic or other medium and retrievable in perceivable form.

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

(A) racial or ethnic origin, religious belief, gender, sexual orientation, citizenship, or immigration status;

(B) credentials sufficient to access an account remotely;

(C) a credit or debit card number or financial account number;

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

(E) geolocation in real time;

(F) a criminal record;

(G) income;

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

(I) genetic sequencing information; or

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

(18) "Sign" means, with present intent to authenticate or adopt a record:

(A) execute or adopt a tangible symbol; or

(B) attach to or logically associate with the record an electronic symbol, sound, or procedure.

(19) "Stakeholder" means a person that has, or represents a person that has, a direct interest in the development of a voluntary consensus standard.

(20) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any other territory or possession subject to the jurisdiction of the United States. The term includes a federally recognized Indian tribe.

(21) "Third-party controller" means a controller that receives from another controller authorized access to personal data or pseudonymized data and determines the purpose and means of additional processing.

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 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 4. Controller and Processor Responsibilities; General Provisions

(a) A controller shall:

(1) if a collecting controller, provide under Section 5 a copy of a data subject's personal data to the data subject on request;

(2) correct or amend a data subject's personal data on the data subject's request under Section 5;

(3) provide notice and transparency under Section 6 about the personal data it maintains and its processing practices;

(4) obtain consent for processing that is an incompatible data practice under Section 8;

(5) abstain from using a prohibited data practice;

(6) conduct and maintain data privacy and security risk assessments under Section 10; and

(7) provide redress for an incompatible data practice or prohibited data practice the controller performs or is responsible for performing while processing a data subject's personal data.

(b) A processor shall:

(1) on request of the controller, provide the controller with a data subject's personal data or enable the controller to access the personal data at no cost to the controller;

(2) correct an inaccuracy in a data subject's personal data on request of the controller;

(3) abstain from processing personal data for a purpose other than one requested

by the controller;

(4) conduct and maintain data privacy and security risk assessments in accordance with Section 10; and

(5) provide redress for an incompatible or prohibited data practice the processor knowingly performs in the course of processing a data subject's personal data at the direction of the controller.

(c) A controller or processor is responsible under this [act] for an incompatible data practice or prohibited data practice committed by another if:

(1) the practice is committed with respect to personal data collected by the controller or processed by the processor; and

(2) the controller or processor knew the personal data would be used for the practice and was in a position to prevent it.

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:

(1) establish a reasonable procedure for a data subject to request, receive a copy of, and propose an amendment or correction to personal data about the data subject;

(2) establish a procedure to authenticate the identity of a data subject who requests a copy of the data subject's personal data;

(3) comply with a request from an authenticated data subject for a copy of personal data about the data subject [not later than 45 days] [within a reasonable time] after receiving it or provide an explanation of action being taken to comply with the request;

(4) on request, provide the data subject one copy of the data subject's personal data free of charge once every 12 months and additional copies on payment of a fee reasonably based on administrative costs;

(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

(6) confirm to the data subject that an amendment or correction has been made or explain why the amendment or correction has not been made.

(b) A collecting controller shall make a reasonable effort to ensure that a correction of personal data performed by the controller also is performed on personal data maintained by a third-party controller or processor that directly or indirectly received personal data from the collecting controller. A third-party controller or processor shall make a reasonable effort to assist the collecting controller, if necessary to satisfy a request of a data subject under this section.

(c) A controller may not deny a good or service, charge a different rate, or provide a different level of quality to a data subject in retaliation for exercising a right under this section. It is not retaliation under this subsection for a controller to make a data subject ineligible to participate in a program if:

(1) the corrected information requested by the data subject makes the data subject ineligible for the program; and

(2) the program's terms of service specify the eligibility requirements for all participants.

(d) An agreement that waives or limits a right or duty under this section is unenforceable.

Section 6. Privacy Policy

(a) A controller shall adopt and comply with a reasonably clear and accessible privacy

policy that discloses:

(1) categories of personal data maintained by or on behalf of the controller;

(2) categories of personal data the controller provides to a processor or another controller and the purpose of providing the personal data;

(3) compatible data practices applied routinely to personal data by the controller or by an authorized processor;

(4) incompatible data practices that, unless the data subject withholds consent, will be applied by the controller or an authorized processor to personal data;

(5) the procedure for a data subject to exercise a right under Section 5;

(6) federal, state, or international privacy laws or frameworks with which the controller complies; and

(7) any voluntary consensus standard adopted by the controller.

(b) The privacy policy under subsection (a) must be reasonably available to a data subject at the time personal data is collected about the subject.

(c) If a controller maintains a public website, the controller shall publish the privacy policy on the website.

Section 7. Compatible Data Practice

(a) A controller or processor may engage in a compatible data practice without the data subject's consent. A controller or processor engages in a compatible data practice if the processing is consistent with the ordinary expectations of data subjects or is likely to benefit data subjects substantially. The following factors apply to determine whether processing is a compatible data practice:

(1) the data subject's relationship with the controller;

(2) the type of transaction in which the personal data was collected;

(3) the type and nature of the personal data that would be processed;

(4) the risk of a negative consequence on the data subject by the use or disclosure of the personal data;

(5) the effectiveness of a safeguard against unauthorized use or disclosure of the personal data; and

(6) the extent to which the practice advances the economic, health, or other interests of the data subject.

(b) A compatible data practice includes processing that:

(1) initiates or effectuates a transaction with a data subject with the subject's knowledge or participation;

(2) is reasonably necessary to comply with a legal obligation or regulatory oversight of the controller;

(3) meets a particular and explainable managerial, personnel, administrative, or operational need of the controller or processor;

(4) permits appropriate internal oversight of the controller or external oversight by a government unit or the controller's or processor's agent;

(5) is reasonably necessary to create pseudonymized or deidentified data;

(6) permits analysis for generalized research or for the research and development of a 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.

(7) is reasonably necessary to prevent, detect, investigate, report on, prosecute, or remediate an actual or potential:

(A) fraud;

(B) unauthorized transaction or claim;

(C) security incident;

(D) malicious, deceptive, or illegal activity;

(E) legal liability of the controller; or

(F) threat to national security;

(8) assists a person or government entity acting under paragraph (7);

(9) is reasonably necessary to comply with or defend a legal claim; or

(10) any other purpose determined to be a compatible data practice under subsection (a).

(c) A controller may use personal data, or disclose pseudonymized data to a third-party controller, to deliver targeted advertising and other purely expressive content to a data subject. Under this subsection a controller may not use personal data or disclose pseudonymized data to be used to offer terms, including terms relating to price or quality, to a data subject that are different from terms offered to data subjects generally. Processing personal data or pseudonymized data for differential treatment is an incompatible data practice unless the processing is otherwise compatible under this section. This subsection does not prevent providing special considerations to members of a program if the program's terms of service specify the eligibility requirements for all participants.

(d) A controller or processor may process personal data in accordance with the rules of a voluntary consensus standard under Sections 12 through 14 unless a court has prohibited the

processing or found it to be an incompatible data practice. To permit processing under a voluntary consensus standard, a controller must commit to the standard in its privacy policy.

Section 8. Incompatible Data Practice

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

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

(2) is otherwise a compatible data practice but is inconsistent with a privacy policy adopted under Section 6.

(b) A controller may process personal data that does not include sensitive data using an incompatible data practice if at the time personal data is collected about a data subject, the controller provides the data subject with notice and information sufficient to allow the data subject to understand the nature of the incompatible data processing and a reasonable opportunity to withhold consent to the practice.

(c) A controller may not process a data subject's sensitive data for an incompatible data practice without the data subject's express consent in a signed record for each practice.

(d) Unless processing is a prohibited data practice, a controller may require a data subject to consent to an incompatible data practice as a condition for access to the controller's goods or services. The controller may offer a reward or discount in exchange for the data subject's consent to process the subject's personal data.

Section 9. Prohibited Data Practice

(a) A controller may not engage in a prohibited data practice. Processing personal data is a prohibited data practice if the processing is likely to:

(1) subject a data subject to specific and significant:

(A) financial, physical, or reputational harm;

(B) embarrassment, ridicule, intimidation, or harassment; or

(C) physical or other intrusion on solitude or seclusion if the intrusion would be highly offensive to a reasonable person;

(2) result in misappropriation of personal data to assume another's identity;

(3) constitute a violation of other law, including federal or state law against discrimination;

(4) fail to provide reasonable data-security measures, including appropriate administrative, technical, and physical safeguards to prevent unauthorized access; or

(5) process without consent under Section 8 personal data in a manner that is an incompatible data practice.

(b) It is a prohibited data practice to collect or create personal data by reidentifying or causing the reidentification of pseudonymized or deidentified data unless:

(1) the reidentification is performed by a controller or processor that previously had pseudonymized or deidentified the personal data;

(2) the data subject expects the personal data to be maintained in identified form by the controller performing the reidentification; or

(3) the purpose of the reidentification is to assess the privacy risk of deidentified data and the person performing the reidentification does not use or disclose reidentified personal data except to demonstrate a privacy vulnerability to the controller or processor that created the deidentified data.

Section 10. Data Privacy and Security Risk Assessment

(a) A controller or processor shall conduct and maintain in a record a data privacy and

security risk assessment. The assessment may take into account the size, scope and type of business of the controller or processor and the resources available to it. The assessment must evaluate:

(1) privacy and security risks to the confidentiality and integrity of the personal data being processed or maintained, the likelihood of the risks, and the impact that the risks would have on the privacy and security of the personal data;

(2) efforts taken to mitigate the risks; and

(3) the extent to which the data practices comply with this [act].

(b) A controller or processor shall update the data privacy and security risk assessment 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.

(c) A data privacy and security risk assessment is confidential and is not subject to [cite to public records laws and discovery rules in a civil action]. The fact that a controller or processor conducted an assessment, the records analyzed in the assessment, and the date of the assessment are not confidential under this section.

Legislative Note: *The state should include appropriate language in subsection (c) exempting a data privacy assessment from an open records request and discovery in a civil case to the maximum extent possible under state law.*

Section 11. Compliance with Other Law Protecting Personal Data

(a) A controller or processor complies with this [act] if it complies with a comparable personal-data protection law in another jurisdiction and the [Attorney General] determines the law in the other jurisdiction is equally or more protective of personal data than this [act]. The [Attorney General] may set a fee to be charged to a controller or processor that asserts compliance with a comparable law under this subsection. The fee must reflect the cost reasonably expected to be

incurred by the [Attorney General] to determine whether the comparable law is equally or more protective than this [act].

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

(1) the Health Insurance Portability and Accountability Act, Pub. L. 104-191, if the controller or processor is regulated by that act;

(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;

(3) the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801 et. seq.;

(4) the Drivers Privacy Protection Act of 1994, 18 U.S.C. Section 2721 et seq.;

(5) the Family Education Rights and Privacy Act of 1974, 20 U.S.C. Section 1232g; or

(6) the Children's Online Privacy Protection Act of 1998, 15 U.S.C. Section 6501 et seq.

Legislative Note: *It is the intent of this act to incorporate future amendments to the cited federal laws. In a state in which the constitution or other law does not permit incorporation of future amendments when a federal statute is incorporated into state law, the phrase "as amended" should be omitted. The phrase also should be omitted in a state in which, in the absence of a legislative declaration, future amendments are incorporated into state law.*

Section 12. Compliance with Voluntary Consensus Standard

A controller or processor complies with a requirement of this [act] if it adopts and complies with a voluntary consensus standard that addresses that requirement and is recognized by the [Attorney General] under Section 15.

Section 13. Content of Voluntary Consensus Standard

A stakeholder may initiate the development of a voluntary consensus standard for compliance with this [act]. A voluntary consensus standard may address any requirement including:

(1) identification of compatible data practices for an industry;

(2) the procedure and method for securing consent of a data subject for an incompatible data practice;

(3) a common method for responding to a request by a data subject for access to or correction of personal data, including a mechanism for authenticating the identity of the data subject;

(4) a format for a privacy policy to provide consistent and fair communication of the policy to data subjects;

(5) practices that provide reasonable security for personal data maintained by a controller or processor; and

(6) any other policy or practice that relates to compliance with this [act].

Section 14. Procedure for Development of Voluntary Consensus Standard

The [Attorney General] may not recognize a voluntary consensus standard unless it is developed through a consensus procedure that:

(1) achieves general agreement, but not necessarily unanimity, and:

(A) includes stakeholders representing a diverse range of industry, consumer, and public interests;

(B) gives fair consideration to each comment by a stakeholder;

(C) responds to each good-faith objection by a stakeholder;

(D) attempts to resolve each good-faith objection by a stakeholder;

(E) provides each stakeholder an opportunity to change the stakeholder's vote after reviewing comments; and

(F) informs each stakeholder of the disposition of each objection and the reason for the disposition;

(2) provides stakeholders a reasonable opportunity to contribute their knowledge, talents, and efforts to the development of the standard;

(3) is responsive to the concerns of all stakeholders;

(4) consistently complies with documented and publicly available policies and procedures that provide adequate notice of meetings and standards development; and

(5) includes a right for a stakeholder to file a statement of dissent.

Section 15. Recognition of Voluntary Consensus Standard

(a) On filing of a request by any person, the [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] finds the standard:

(1) does not conflict with any requirement of Sections 5 through 10;

(2) is developed through a procedure that substantially complies with Section 14; and

(3) reasonably reconciles a requirement of this [act] with the requirements of other law.

(b) The [Attorney General] shall adopt rules under [cite to state administrative procedure act] or otherwise establish a procedure for filing a request under subsection (a). The rules may:

(1) require that the request be in a record demonstrating that the standard and procedure through which it was adopted comply with this [act];

(2) require the applicant to indicate whether the standard has been recognized as

appropriate elsewhere and, if so, identify the authority that recognized it; and

(3) set a fee to be charged to the applicant, which must reflect the cost reasonably expected to be incurred by the [Attorney General] in acting on a request.

(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.

(d) After notice and hearing, the [Attorney General] may withdraw recognition of a voluntary consensus standard if the [Attorney General] finds that the standard or its implementation is not consistent with this [act].

(e) A voluntary consensus standard recognized by the [Attorney General] is a public record under [cite to state public records law].

Section 16. Applicability of [Consumer Protection Act]

(a) The enforcement authority, remedies, and penalties provided by the [cite to state consumer protection act] apply to a violation of this [act].

(b) The [Attorney General] may adopt rules under [cite to state administrative procedure act] to implement this [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 uniformity among the states consistent with this [act]. The [Attorney General] may:

(1) consult with Attorneys General or other personal-data-privacy-enforcement agencies in other jurisdictions that have an act substantially similar to this [act];

(2) consider suggested or model rules or enforcement guidelines promulgated by the National Association of Attorneys General or any successor organization;

(3) consider the rules and practices of Attorneys General or other personal-data-privacy-enforcement agencies in other jurisdictions; and

(4) consider voluntary consensus standards developed consistent with this [act], that have been recognized by other Attorneys General or other personal-data-privacy-enforcement agencies.

[(d) In an action or proceeding to enforce this [act] by the [Attorney General] in which the [Attorney General] prevails, the [Attorney General] may recover reasonable expenses and costs incurred in investigation and prosecution of the case.]

[(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) 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*

Section 17. Limits of Act

This [act] does not create or affect a cause of action under other law of this state.

Section 18. Uniformity of Application and Construction

In applying and construing this uniform act, a court shall consider the promotion of uniformity of the law among jurisdictions that enact it.

Section 19. Electronic Records and Signatures in Global and National Commerce Act

This [act] modifies, limits, or supersedes the Electronic Signatures in Global and National

Commerce Act, 15 U.S.C. Section 7001 et seq.[as amended], but does not modify, limit, or supersede 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in 15 U.S.C. Section 7003(b).

[Section 20. Severability

If a provision of this [act] or its application to a person or circumstance is held invalid, the invalidity does not affect another provision or application that can be given effect without the invalid provision.]

Legislative Note: *Include this section only if the state lacks a general severability statute or a decision by the highest court of this state adopting a general rule of severability.*

Section 21. Effective Date

This [act] takes effect [180 days after the date of enactment].

Legislative Note: *A state may wish to include a delayed effective date to allow time for affected agencies and industry members to prepare for implementation and compliance.*