DRAFT

FOR DISCUSSION ONLY

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

February 21–22, 2020 Drafting Committee Meeting

Copyright © 2020
By
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the drafting committee. They do not necessarily reflect the views of the Conference and its commissioners and the drafting committee and its members and reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

January 7, 2020

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

The committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

HARVEY S. PERLMAN	Nebraska, *Chair*
JAMES BOPP JR.	Indiana
STEPHEN Y. CHOW	Massachusetts
PARRELL D. GROSSMAN	North Dakota
JAMES C. McKAY JR.	District of Columbia
LARRY METZ	Florida
JAMES E. O'CONNOR	Nebraska
ROBERT J. TENNESSEN	Minnesota
KERRY TIPPPER	Colorado
ANTHONY C. WISNIEWSKI	Maryland
CANDACE M. ZIERDT	Florida
DAVID V. ZVENYACH	Wisconsin
CARL H. LISMAN	Vermont, *President*
WILLIAM H. HENNING	Alabama, *Division Chair*

OTHER PARTICIPANTS

WILLIAM McGEVERAN	Minnesota, *Reporter*
MICHAEL AISENBERG	Virginia, *American Bar Association Advisor*
STEVEN L. WILLBORN	Nebraska, *Style Liaison*
TIM SCHNABEL	Illinois, *Executive Director*

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

TABLE OF CONTENTS

COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

SECTION 1. SHORT TITLE. This [act] may be cited as the Collection and Use of Personally Identifiable Data Act.

SECTION 2. DEFINITIONS. In this [act]

(1) "Data controller" or "controller" means a data custodian who, alone or jointly with others, decides upon the purposes, means, and extent of processing to be conducted in relation to personal data that has been in its possession or control.

(2) "Data custodian" or "custodian" means a person in possession or control of personal data or deidentified data. Controllers and processors are data custodians.

(3) "Data processor" or "processor" means a data custodian who processes personal data on behalf of a data controller and under that data controller's direction.

(4) "Data subject" means the individual, device, or household to whom personal data refers.

(5) "Deidentified" means that the capacity of information to identify, describe, or be associated with any particular individual, device, or household has been eliminated, provided the custodian of the information makes no attempt to reidentify the information and implements all of the following:

(A) Technical safeguards that reasonably prevent reidentification of the individual, device, or household to whom the information may pertain.

(B) Business processes that specifically prohibit reidentification of the information; and

(C) Business processes that reasonably prevent inadvertent release of deidentified data.

(6) “Device” means any physical object that connects to the internet or to another device.

(7) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

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

(9) “Personal data” means information that identifies or describes a particular individual, household, or device, and information that can be associated with a particular individual, household, or device by using a reasonable amount of effort. Personal data need not have been collected directly from a data subject. Probabilistic inferences about an individual, household, or device, including inferences derived from profiling, are included in the definition of personal data. Deidentified data and publicly available data are not personal data.

(10) “Processing” means any operation performed on personal data, whether or not by automated means, including use, storage, disclosure, analysis, and modification.

(11) “Profiling” means any form of automated processing of personal data to evaluate, analyze, or predict a data subject’s economic status, health, demographic characteristics (including race, gender, or sexual orientation), personal preferences, interests, character, reliability, behavior, social or political views, physical location, or movements. Profiling does not include evaluation, analysis, or prediction based solely on a data subject’s current activity, including search queries, if no personal data is retained for future use after the completion of the activity. Probabilistic inferences derived from profiling are personal data.

(12) “Publicly available data” means information that has been made available from federal, state, or local government records in accordance with law, provided the information is

being used in a manner consistent with any conditions on its use imposed by law.

(13) "Sensitive data" means

(A) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, activities or preferences related to gender or sexuality, or citizenship or immigration status;

(B) biometric and genetic data; and

(C) personal data about a data subject who is known to be under [13] years of age.

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

(A) to execute or adopt a tangible symbol; or

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

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

(16) "Targeted advertising" means advertising displayed to a data subject on the basis of profiling.

(17) "Transfer" means to convey personal data into the possession or control of another custodian.

SECTION 3. SCOPE.

(a) This [law] applies to the commercial activities of a person who conducts business [in the State of X] or produces products or provides services targeted to [the State of X], provided that the person:

(1) is the custodian of personal data concerning more than [50,000] individuals,

devices, or households in one year,

(2) earns more than [50] percent of its gross annual revenue directly from its activities as a controller or processor of personal data, or

(3) is a data processor acting on behalf of a data controller whose activities satisfy the requirements of this section.

(b) This [act] does not apply to personal health information as defined under the Health Information Portability and Accountability Act [CITE] [and regulations] when the custodian of that data is regulated by that statute.

(c) This [act] does not apply to the activities of a consumer reporting agency as defined under [FCRA] in connection with activities regulated by that statute.

(d) This [act] does not apply to state or local government entities.

Reporter's Note: Other exclusions from scope?

SECTION 4. DUTIES ACCORDING TO ROLE. A data custodian shall be responsible for the duties in Sections 5-9. A data controller shall be responsible for the additional duties in Sections 10-11 and for the satisfaction of data subject rights in Sections 12-17.

(a) Processing by the processor shall be governed by a written contract between the controller and processor that is binding on both parties and that sets out the nature and purpose of the processing, the type of personal data subject to the processing (including the identification of any sensitive data), the duration of the processing, and the obligations and rights of both parties.

(b) A data processor shall adhere to the instructions of the data controller and shall assist the controller in fulfilling its duties under this [act].

(c) A data processor shall not process personal data for any purpose that was not included in the notice provided to data subjects by the data controller as required by this [act].

(d) A data processor shall make available to the data controller all information necessary to demonstrate the processor's compliance with the requirements of this [act] and with the requirements of the contract between the controller and processor. The contract shall give the controller a reasonable right to audit the conduct of the processor in relation to the processing.

(e) A data processor may only transfer personal data to another processor or to any other person with the express written consent of the controller. Any such transfer must be governed by a written contract that imposes all the same obligations on the recipient of the personal data that are imposed on the processor in the contract between the controller and the processor, regardless of whether the recipient is otherwise subject to this [act].

(f) A data controller may indemnify a data processor for liability of the data processor under this [act].

SECTION 5. DESIGNATION OF DATA PRIVACY OFFICER. A data custodian shall designate an individual employee or contractor to serve as the custodian's data privacy officer.

(a) A data privacy officer shall have qualifications appropriate for the supervision of the custodian's responsibilities under this [act]. Minimum qualifications shall depend on the scale, complexity, and risks of the data processing activities undertaken by the custodian.

(b) A data privacy officer shall be responsible for the data privacy assessments required by this [act] and shall sign each data privacy assessment personally.

(c) A data privacy officer may perform other duties for the custodian or for other persons, provided the data privacy officer spends a reasonably sufficient amount of time directing a custodian's duties under [this law]. If a data privacy officer is not an employee of the custodian, the custodian and the data privacy officer must execute a written agreement that clearly specifies the data privacy officer’s duties. An individual may serve as a data privacy officer for more than one data custodian.

(d) A data privacy officer may assign or delegate other persons to complete tasks under supervision, but the data privacy officer must retain authority over the completion of those tasks.

SECTION 6. DATA PRIVACY ASSESSMENT. A custodian must conduct, to the extent not previously conducted, a written data privacy assessment of each data processing activity undertaken by the custodian, in order to evaluate all material risks, harms, and benefits of processing.

(a) A data privacy assessment shall be completed about each data processing activity every two years. It shall be updated any time a change in processing activities may materially increase privacy risks to data subjects.

(b) A data privacy assessment shall evaluate

(1) the type of personal data being processed;

(2) the presence of any sensitive data among the personal data being processed;

(3) the scale of the processing activities;

(4) the context in which personal data is collected and processed;

(5) the seriousness of privacy risks imposed on data subjects as a result of the processing;

(6) the likelihood of privacy risks causing harm to data subjects as a result of the processing;

(7) the benefits that may flow directly or indirectly to the custodian, data subjects, the public, or others as a result of the processing;

(8) the resources reasonably available to the data custodian for addressing privacy

risks, taking account of the revenue generated by the processing; and

(9) the measures the custodian has undertaken to mitigate any privacy risks.

(c) Privacy risks evaluated in a data privacy assessment shall encompass risks of all potential harms to data subjects, including

(1) accidental disclosure, theft, or other breaches of security causing personal data to be revealed to persons without authorization;

(2) identity theft;

(3) harassment;

(4) unwanted profiling;

(5) stigmatization or reputational harm;

(6) emotional harm including anxiety, embarrassment, fear, and other demonstrable mental harms; and

(7) other foreseeable outcomes that would be highly offensive to the reasonable person.

(d) A data processor may adopt data privacy assessments completed by a data controller concerning the same personal data, provided the assessment satisfies all requirements of this section.

(e) A data custodian must retain a written copy of all data privacy assessments for ten years after their completion. Upon request of the [Attorney General] in connection with [an investigation], a data custodian must provide copies of all current and former data privacy assessments.

(f) Whether or not a data custodian has provided data privacy assessments to the Attroney General, a data privacy assessment is confidential business information [and is not subject to public records requests or subject to compulsory civil discovery in any court].

Legislative Note: *The state should include appropriate language in subsection 6(f) exempting data privacy assessments from open records requests and compulsory civil discovery requests to the maximum extent possible under state law.*

SECTION 7. CUSTODIAN'S DUTY OF LOYALTY. A data custodian shall not

(a) process or use personal data when processing or use exposes a data subject to reasonably foreseeable and material risks and harms that are not outweighed by benefits to the data subject or the public, or

(b) engage in processing practices that are unfair, deceptive, or abusive.

SECTION 8. CUSTODIAN'S DUTY OF DATA SECURITY. A data custodian shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in the custodian's possession or control. Reasonable data security measures shall include administrative, technical, and physical safeguards as appropriate. Data security measures shall be evaluated as part of the data privacy assessment required under this [act]. An evaluation of the reasonableness of data security measures shall take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the custodian, and industry practices among other custodians who are similarly situated. Reasonable security practices may be derived from best practices promulgated by professional organizations, government entities, or other specialized sources.

SECTION 9. CUSTODIAN'S DUTY OF DATA MINIMIZATION. A data custodian shall not collect, process, or retain more personal data than necessary to achieve the purposes of processing. When a data controller transfers personal data to a data processor, the controller shall transfer and the processor shall accept only as much personal data as is necessary to complete the processor's processing activities. At the completion of processing, a processor shall destroy all personal data or return it to the controller, pursuant to the agreement between the controller and processor required under section 4.

SECTION 10. CONTROLLER'S DUTY OF TRANSPARENCY.

(a) A data controller shall provide data subjects with a reasonably accessible, clear, and meaningful privacy notice which discloses

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

(2) the purposes for processing of personal data, either by the controller or on the controller's behalf;

(3) the categories of personal data that the controller provides to processors or to any other persons;

(4) the categories of processors or other persons who receive personal data from the controller;

(5) the nature and purpose of any profiling of data subjects conducted using the personal data; and

(6) the means by which a data subject may exercise rights provided by this [act].

(b) The notice under this section shall clearly and conspicuously designate at least two methods for a data subject to contact the data controller in order to exercise rights under this [act]. At least one of these methods shall be a toll-free telephone number. If the controller maintains an internet web site, at least one of these methods shall be contact through the web site.

(c) If the data controller processes personal data for targeted advertising, or provides personal data to any processor or other person to process for targeted advertising, the notice under this section shall clearly and conspicuously disclose such processing and shall provide an automated internet-based mechanism for the data subject to exercise the right to opt out of targeted advertising under this [act].

(d) The notice under this section shall be reasonably available at the time personal data is collected from a data subject.

SECTION 11. CONTROLLER'S DUTY OF PURPOSE LIMITATION. A controller shall not process personal data, or permit processors or other persons to process personal data, for purposes that are not specified in the notice to data subjects required by this [act].

SECTION 12. DATA SUBJECT RIGHTS GENERALLY.

(a) A data subject may exercise rights under sections 13-16 by notifying the controller by any reasonable means of the data subject's intent to exercise one or more of these rights. Parents of a [minor child] may exercise these rights on behalf of the [minor child]. If personal data pertains to a household or device, a person who belongs to the household or owns the device may identify the household or device and exercise the rights specified under this [act] in relation to personal data about that household or device.

(b) A data controller shall comply with requests without undue delay. If the data controller has not complied with the request within 45 days of receiving it, the data controller shall notify the data subject who made the request and shall provide an explanation of the actions being taken to comply with the request.

(c) A data controller shall make reasonable efforts to ensure that its responses to requests by data subjects to exercise rights under this [act] include personal data in the possession or control of data processors acting on the controller's behalf. The data controller shall make reasonable efforts to notify processors acting on its behalf when a data subject exercises these rights, and shall instruct the processor to comply in the same fashion as the controller.

(d) A data controller shall establish procedures for determining responses to data subjects' assertions of rights under sections 13-16. The data privacy officer for a data controller shall approve such procedures. An explanation of the procedures in clear language shall be reasonably accessible to all data subjects. The procedures shall include an opportunity to appeal an initial determination by the data controller. Appeals of an initial determination shall be reviewed under the supervision of the data privacy officer. If a data subject is dissatisfied with the final disposition of an appeal, the data processor shall inform the data subject of the procedure to [file a complaint] with the [Attorney General].

SECTION 13. RIGHTS OF ACCESS AND PORTABILITY.

(a) A data subject has the right to receive confirmation from a data controller indicating whether the data controller controls or possesses any personal data that the controller knows pertains to the data subject.

(b) A data subject has the right to receive a copy of personal data covered by subsection (a). Once per year, the data controller must provide this copy free of charge. The data controller may charge a reasonable fee based on actual administrative costs to comply with additional requests for copies under this subsection. If requests are manifestly unreasonable or excessive, in particular because of their repetitive character, the data controller may refuse to act on requests from that data subject for one year. The data controller bears the burden of demonstrating that a request is manifestly unreasonable or excessive.

(c) If a data controller collected personal data directly from the data subject, the data controller shall provide the copy in subsection (b) to the data subject in a format that, to the extent technically feasible, is portable and enables the data subject to transmit the personal data to another data controller conveniently and, where applicable, by automated means.

SECTION 14. RIGHTS RELATED TO TARGETED ADVERTISING AND PROFILING.

(a) A data subject has the right to restrict a data controller from processing or transferring personal data pertaining to the data subject (an "opt out") for purposes of

(1) targeted advertising;

(2) profiling in furtherance of decisions that produce legal effects or similarly significant effects concerning the data subject.

(b) If a controller processes or transfers sensitive data for the purposes listed in subsection (a), the controller must receive affirmative consent (an "opt in") from the data subject before undertaking such processing or transfer.

SECTION 15. RIGHT OF CORRECTION. A data subject has the right to require a controller to correct inaccuracies in personal data pertaining to the data subject.

SECTION 16. RIGHT OF DELETION. A data subject has the right to require a controller to delete personal data pertaining to the data subject.

SECTION 17. NONDISCRIMINATION. A data controller shall not discriminate against any data subject for exercising rights under this [act], including by denying goods and services, charging different rates, or providing a different level of quality, except that a data controller may provide benefits to data subjects that are closely related to the purpose of processing and that require access to personal data.

SECTION 18. WAIVERS PROHIBITED. Any provision of a contract or agreement that purports to waive or limit rights or duties imposed by this [act] is contrary to public policy and shall be void and unenforceable, except that a controller may indemnify a processor for liability under this [act].

SECTION 19. REGULATORY ENFORCEMENT. The provisions of this [act] shall be enforced by [the Attorney General].

Legislative Note: *The state should include appropriate language cross-referencing the particular powers of the Attorney General that will be applied to enforcement of this statute and the applicable penalties.*

SECTION 20. PRIVATE RIGHT OF ACTION.

(a) A data subject may bring a civil suit against a data custodian for violations of sections 7, 8, 11, 13, 14, 15, 16, or 17. A private party may not bring suit in state or federal court alleging violation of any other part of this [act].

(b) Damages available to a person in a suit under this section shall be actual damages or damages of [$100], whichever is greater.

(c) Evidence about the development or results of a data privacy assessment is not subject to compulsory discovery in a civil suit brought under this [act], and shall be treated by the court in the same manner as a confidential offer of settlement, unless a data custodian voluntarily introduces evidence related to a data privacy assessment. If a data custodian voluntarily introduces evidence related to a data privacy assessment, admissibility and discoverability of evidence related to that data privacy assessment shall be handled in accordance with the court's ordinary rules of evidence.

SECTION 21. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

**SECTION 22. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND

NATIONAL COMMERCE ACT. This [act] modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001, et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

SECTION 23. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.

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

SECTION 24. EFFECTIVE DATE. This [act] takes effect [180 days] after the date of enactment.