LB1188
2022

LEGISLATURE OF NEBRASKA

ONE HUNDRED SEVENTH LEGISLATURE

SECOND SESSION

LEGISLATIVE BILL 1188

Introduced by Flood, 19.

Read first time January 20, 2022

Committee: Banking, Commerce and Insurance

A BILL FOR AN ACT relating to personal data; to adopt the Uniform Personal Data Protection Act; to provide an operative date; and to provide severability.

Be it enacted by the people of the State of Nebraska,

LB1188
2022

Section 1. Sections 1 to 19 of this act shall be known and may be cited as the Uniform Personal Data Protection Act.

Sec. 2. For purposes of the Uniform Personal Data Protection 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 of this act.

(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 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 of 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, and telephone number.

(7) Incompatible data practice means processing that may be performed consistent with section 8 of this act.

(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 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

LB1188
2022

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 of this act.

(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, browser, software, or hardware identification code, or other data uniquely linked 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 made available lawfully to the general public if:

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

LB1188
2022

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 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 thirteen 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.

LB1188
2022

(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.

Sec. 3. (a) Except as provided in subsections (b) and (c) of this section, the Uniform Personal Data Protection 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) at any time during a calendar year maintains personal data about more than fifty thousand 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 fifty percent of its gross annual revenue during a calendar year from maintaining personal data as a controller or processor;

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

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

(b) The Uniform Personal Data Protection Act does not apply to an agency or instrumentality of this state or a political subdivision of this state.

(c) The Uniform Personal Data Protection Act does not apply to personal data that is:

(1) publicly available information;

(2) processed or maintained solely as part of human-subjects

LB1188
2022

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 sections 84-712 to 84-712.09; or

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

Sec. 4. (a) A controller shall:

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

(2) correct or amend under section 5 of this act a data subject's personal data on the data subject's request;

(3) provide notice under section 6 of this act about the personal data it maintains and its processing practices;

(4) obtain consent under section 8 of this act for processing that is an incompatible data practice;

(5) not use a prohibited data practice;

(6) conduct and maintain under section 10 of this act data-privacy and security-risk assessments; and

(7) provide redress for a 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) on request of the controller, correct an inaccuracy in a data subject's personal data;

(3) not process personal data for a purpose other than one requested

LB1188
2022

by the controller;

(4) conduct and maintain data-privacy and security-risk assessments in accordance with section 10 of this act; and

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

(c) A controller is responsible under the Uniform Personal Data Protection Act for a prohibited data practice conducted by another if:

(1) the practice is conducted with respect to personal data collected by the controller; and

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

(d) A processor is responsible under the Uniform Personal Data Protection Act for a prohibited data practice or conducted by another if:

(1) the practice is conducted with respect to personal data processed by the processor; and

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

Sec. 5. (a) Unless personal data is pseudonymized and not maintained with sensitive data, a 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) not later than forty-five days after receiving a request from a data subject authenticated under subdivision (2) of this subsection for a copy of personal data about the data subject, comply with the request or provide an explanation of action being taken to comply with it;

LB1188
2022

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

(5) make an amendment or correction requested by a data subject if the collecting 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 the 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 data subject 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) 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.

Sec. 6. (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;

LB1188
2022

(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, if the data subject consents under section 8 of this act, will be applied by the controller or an authorized processor;

(5) the procedure for a data subject to request a copy of, or propose an amendment or correction to, personal data under section 5 of this act;

(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) of this section must be reasonably available to a data subject at the time personal data is collected about the data subject.

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

Sec. 7. (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 processed;

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

LB1188
2022

(5) the effectiveness of safeguards 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 data 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 by the controller's or processor's agent or external oversight by a government unit;

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

(6) permits analysis:

(A) 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; or

(B) for research and development of a product or service;

(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 processor; or

(F) threat to national security;

(8) assists a person or government entity acting under subdivision

LB1188
2022

(7) of this subsection;

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

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

(c) A controller may use personal data, or disclose pseudonymized data to a third-party controller, to deliver to a data subject targeted advertising and other purely expressive content. A controller may not use personal data, or disclose pseudonymized data, to offer terms to a data subject that are different from terms offered to data subjects generally, including terms relating to price or quality. 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 different treatment 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 to 15 of this act unless a court has prohibited the processing or found it to be an incompatible data practice. Processing under a voluntary consensus standard is permitted only if a controller adopts and commits to the standard in its privacy policy.

Sec. 8. (a) A controller or processor engages in an incompatible data practice if the processing:

(1) is not a compatible data practice under section 7 of this act or a prohibited data practice under section 9 of this act; or

(2) even if a compatible data practice under section 7 of this act, is inconsistent with a privacy policy adopted under section 6 of this act.

(b) A controller may use an incompatible data practice to process personal data that does not include sensitive data if, at the time the

LB1188
2022

personal data is collected about a data subject, the controller provides the data subject:

(1) notice and information sufficient to allow the data subject to understand the nature of the incompatible data processing; and

(2) a reasonable opportunity to withhold consent to the practice.

(c) A controller may not process a data subject's sensitive data using 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 data subject's personal data.

Sec. 9. (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 of this act personal data in a manner that is an incompatible data practice.

(b) Reidentifying or causing the reidentification of pseudonymized

LB1188
2022

or deidentified data is a prohibited data practice 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.

Sec. 10. (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 the Uniform Personal Data Protection 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 sections 84-712 to 84-712.09 and Chapter 25, article 12. 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.

LB1188
2022

Sec. 11. (a) A controller or processor complies with the Uniform Personal Data Protection Act if it complies with a comparable law protecting personal data in another jurisdiction and the Attorney General determines the law in the other jurisdiction is at least as protective of personal data as the Uniform Personal Data Protection Act. The Attorney General may charge a fee to a controller or processor that requests a determination of 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 at least as protective as the Uniform Personal Data Protection Act.

(b) A controller or processor complies with the Uniform Personal Data Protection Act with respect to processing that is subject to the following acts, as such acts existed on January 1, 2022:

(1) the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, if the controller or processor is regulated by that act;

(2) the Fair Credit Reporting Act, 15 U.S.C. 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. 1681a(f), a furnisher of the information, or a person procuring or using a consumer report;

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

(4) the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq.;

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

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

Sec. 12. A controller or processor complies with a requirement of the Uniform Personal Data Protection 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 of this act.

LB1188
2022

Sec. 13. A stakeholder may initiate the development of a voluntary consensus standard for compliance with the Uniform Personal Data Protection 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 a copy or correction of personal data, including a mechanism for authenticating the identity of the data subject;

(4) a format for a privacy policy that provides 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 the Uniform Personal Data Protection Act.

Sec. 14. 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 position 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;

LB1188
2022

(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) permits a stakeholder to file a statement of dissent.

Sec. 15. (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 to 10 of this act;

(2) is developed through a procedure that substantially complies with section 14 of this act; and

(3) if necessary, reasonably reconciles a requirement of the Uniform Personal Data Protection Act with the requirements of other law.

(b) The Attorney General shall adopt rules under the Administrative Procedure Act or otherwise establish a procedure for filing a request under subsection (a) of this section. The rules may require:

(1) that the request be in a record demonstrating the standard and procedure through which it was adopted comply with the Uniform Personal Data Protection Act;

(2) the person filing the request to indicate whether the standard has been recognized as appropriate in another jurisdiction and, if so, identify the authority that recognized it; and

(3) the person filing the request to pay a fee, 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 the

LB1188
2022

Uniform Personal Data Protection 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 the Uniform Personal Data Protection Act.

(e) A voluntary consensus standard recognized by the Attorney General is a public record under section 84-712 to 84-712.09.

Sec. 16. (a) Subject to subsection (e) of this section, the enforcement authority, remedies, and penalties provided by the Consumer Protection Act apply to a violation of the Uniform Personal Data Protection Act.

(b) The Attorney General may adopt rules under the Administrative Procedure Act to implement the Uniform Personal Data 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 uniformity among the states. The Attorney General may:

(1) consult with Attorneys General and other agencies with authority to enforce personal-data privacy in other jurisdictions that have laws substantially similar to the Uniform Personal Data Protection Act;

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

(3) consider the rules and practices of Attorneys General and other agencies with authority to enforce personal-data privacy in other jurisdictions; and

(4) consider voluntary consensus standards developed consistent with the Uniform Personal Data Protection Act, that have been recognized by other Attorneys General or other agencies with authority to enforce personal-data privacy.

LB1188
2022

(d) In an action or proceeding to enforce the Uniform Personal Data Protection 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 action or proceeding.

(e) A private cause of action for a violation of the Uniform Personal Data Protection Act is not authorized by the Uniform Personal Data Protection Act or the Consumer Protection Act.

Sec. 17. The Uniform Personal Data Protection Act does not create or affect a cause of action under other law of this state.

Sec. 18. In applying and construing the Uniform Personal Data Protection Act, a court shall consider the promotion of uniformity of the law among jurisdictions that enact it.

Sec. 19. The Uniform Personal Data Protection Act modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001 et seq., as such act existed on January 1, 2022, but does not modify, limit, or supersede 15 U.S.C. 7001(c), or authorize electronic delivery of any of the notices described in 15 U.S.C. 7003(b).

Sec. 20. This act becomes operative on January 1, 2023.

Sec. 21. If any section in this act or any part of any section is declared invalid or unconstitutional, the declaration shall not affect the validity or constitutionality of the remaining portions.