LB1294
2024

LEGISLATURE OF NEBRASKA

ONE HUNDRED EIGHTH LEGISLATURE

SECOND SESSION

LEGISLATIVE BILL 1294

Introduced by Bostar, 29; Aguilar, 35; Ballard, 21; Jacobson, 42; von Gillern, 4.

Read first time January 16, 2024

Committee: Banking, Commerce and Insurance

A BILL FOR AN ACT relating to data privacy; to amend sections 71-605.02 and 71-616, Reissue Revised Statutes of Nebraska, section 84-712.05, Revised Statutes Cumulative Supplement, 2022, and section 71-612, Revised Statutes Supplement, 2023; to adopt the Data Privacy Act; to change provisions relating to the preservation and use of certain certificates and information relating to vital records; to provide for certain records to be exempt from public disclosure; to provide an operative date; to provide severability; and to repeal the original sections.

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

LB1294
2024

Section 1. Sections 1 to 30 of this act shall be known and may be cited as the Data Privacy Act.

Sec. 2. For purposes of the Data Privacy Act:

(1) Affiliate means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For purposes of this subdivision, control or controlled means:

(a) The ownership of, or power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company;

(b) The control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(c) The power to exercise controlling influence over the management of a company;

(2) Authenticate means to verify through reasonable means that the consumer who is entitled to exercise the consumer's rights under sections 7 to 11 of this act is the same consumer exercising those consumer rights with respect to the personal data at issue;

(3)(a) Biometric data means data that is used to identify a specific individual through an automatic measurement of a biological characteristic of an individual and includes any:

(i) Fingerprint;

(ii) Voice print;

(iii) Retina image;

(iv) Iris image;

(v) Information derived from wastewater; or

(vi) Unique biological pattern or characteristic; and

(b) Biometric data does not include a physical or digital photograph; a video or audio recording or data generated from a physical or digital photograph; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act;

LB1294
2024

(4) Business associate has the meaning assigned to the term by the Health Insurance Portability and Accountability Act;

(5) Child means an individual younger than thirteen years of age;

(6)(a) Consent means, when referring to a consumer, a clear and affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer, and includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

(b) Consent, when referring to a consumer, does not include:

(i) Acceptance of a general or broad term of use or similar document that contains a description of personal data processing along with other, unrelated information;

(ii) Hovering over, muting, pausing, or closing a given piece of content; or

(iii) Agreement obtained through the use of a dark pattern;

(7)(a) Consumer means an individual who is a resident of this state acting only in an individual or household context.

(b) Consumer does not include an individual acting in a commercial or employment context;

(8) Controller means an individual or other person that, alone or jointly with others, determines the purpose and means of processing personal data;

(9) Covered entity has the same meaning as defined in 45 C.F.R. 160.103, as such regulation existed on January 1, 2024;

(10) Dark pattern means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice, and includes any practice determined by the Federal Trade Commission to be a dark pattern as of January 1, 2024;

(11) Decision that produces a legal or similarly significant effect concerning a consumer means a decision made by the controller that results in the provision or denial by the controller of:

LB1294
2024

(a) Financial and lending services;

(b) Housing, insurance, or health care services;

(c) Education enrollment;

(d) Employment opportunities;

(e) Criminal justice; or

(f) Access to basic necessities, such as food and water;

(12) Deidentified data means data that cannot reasonably be linked to an identified or identifiable individual, or a device linked to that individual;

(13) Health care provider has the same meaning as in the Health Insurance Portability and Accountability Act;

(14) Health Insurance Portability and Accountability Act means the federal Health Insurance Portability and Accountability Act of 1996, as such act existed on January 1, 2024;

(15) Health record means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual that concerns the individual and the services provided to such individual, and includes:

(a) The substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services; or

(b) Information otherwise acquired by the health care provider about an individual in confidence and in connection with health care services provided to the individual;

(16) Identified or identifiable individual means a consumer who can be directly or indirectly readily identified;

(17) Institution of higher education means any postsecondary institution or private postsecondary institution as such terms are defined in section 85-2403;

(18) Known child means a child under circumstances where a controller has actual knowledge of, or willfully disregards, the child's

LB1294
2024

age;

(19) Nonprofit organization means any corporation organized under the Nebraska Nonprofit Corporation Act, any organization exempt from taxation under section 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code, any organization exempt from taxation under section 501(c)(4) of the Internal Revenue Code that is established to detect or prevent insurance-related crime or fraud, and any subsidiary or affiliate of a cooperative corporation organized in this state;

(20)(a) Personal data means any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual, and includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual.

(b) Personal data does not include deidentified data or publicly available information;

(21) Political organization means a party, committee, association, fund, or other organization, regardless of whether incorporated, that is organized and operated primarily for the purpose of influencing or attempting to influence:

(a) The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed; or

(b) The election of a presidential or vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed;

(22)(a) Precise geolocation data means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a

LB1294
2024

radius of one thousand seven hundred fifty feet.

(b) Precise geolocation data does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility;

(23) Process or processing means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data;

(24) Processor means a person that processes personal data on behalf of a controller;

(25) Profiling means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements;

(26) Protected health information has the same meaning as in the Health Insurance Portability and Accountability Act;

(27) Pseudonymous data means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual;

(28) Publicly available information means information that is lawfully made available through government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience;

(29)(a) Sale of personal data means the sharing, disclosing, or

LB1294
2024

transferring of personal data for monetary or other valuable consideration by the controller to a third party.

(b) Sale of personal data does not include:

(i) The disclosure of personal data to a processor that processes the personal data on the controller's behalf;

(ii) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(iii) The disclosure or transfer of personal data to an affiliate of the controller;

(iv) The disclosure of information that the consumer:

(A) Intentionally made available to the general public through a mass media channel; and

(B) Did not restrict to a specific audience; or

(v) The disclosure or transfer of personal data to a third party as an asset that is part of a merger or acquisition;

(30) Sensitive data means a category of personal data, and includes:

(a) Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexuality, or citizenship or immigration status;

(b) Genetic or biometric data that is processed for the purpose of uniquely identifying an individual;

(c) Personal data collected from a known child; or

(d) Precise geolocation data;

(31) State agency means a department, commission, board, office, council, authority, or other agency in any branch of state government that is created by the constitution or a statute of this state, including any university system or any postsecondary institution as defined in section 85-2403;

(32)(a) Targeted advertising means displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or

LB1294
2024

online applications to predict the consumer's preferences or interests.

(b) Targeted advertising does not include:

(i) An advertisement that:

(A) Is based on activities within a controller's own websites or online applications;

(B) Is based on the context of a consumer's current search query, visit to a website, or online application; or

(C) Is directed to a consumer in response to the consumer's request for information or feedback; or

(ii) The processing of personal data solely for measuring or reporting advertising performance, reach, or frequency;

(33) Third party means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor;

(34) Trade secret means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(a) The owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and

(b) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Sec. 3. (1) The Data Privacy Act applies only to a person that:

(a) Conducts business in this state or produces a product or service consumed by residents of this state;

LB1294
2024

(b) Processes or engages in the sale of personal data; and

(c) Is not a small business as determined under the federal Small Business Act, as such act existed on January 1, 2024, except to the extent that section 18 of this act applies to a person described by this subdivision.

(2) The Data Privacy Act does not apply to any:

(a) State agency or political subdivision of this state;

(b) Financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., as such title existed on January 1, 2024;

(c) Covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, 45 C.F.R. parts 160 and 164, as such parts existed on January 1, 2024, and Division A, Title XIII, and Division B, Title IV, of the federal Health Information Technology for Economic and Clinical Health Act, Public Law No. 111-5, as such act existed on January 1, 2024;

(d) Nonprofit organization;

(e) Institution of higher education;

(f) Electric supplier or supplier of electricity as defined in section 70-1001.01;

(g) Natural gas public utility as defined in section 66-1802; or

(h) A natural gas utility owned or operated by a city or a metropolitan utilities district.

Sec. 4. The Data Privacy Act does not apply to the following:

(1) Protected health information under the Health Insurance Portability and Accountability Act;

(2) Health records;

(3) Patient identifying information for purposes of 42 U.S.C. 290dd-2, as such section existed on January 1, 2024;

(4) Identifiable private information:

LB1294
2024

(a) For purposes of the federal policy for the protection of human subjects under 45 C.F.R. part 46, as such part existed on January 1, 2024;

(b) Collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, as such guidelines existed on January 1, 2024, or of the protection of human subjects under 21 C.F.R. parts 50 and 56, as such parts existed on January 1, 2024; or

(c) That is personal data used or shared in research conducted in pursuant to the Data Privacy Act or other research conducted in accordance with applicable Nebraska law;

(5) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq., as such act existed on January 1, 2024;

(6) Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21 et seq., as such act existed on January 1, 2024;

(7) Information derived from any of the health care-related information listed in this section that is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act;

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section that is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act or by a program or a qualified service organization as defined by 42 U.S.C. 290dd-2, as such section existed on January 1, 2024;

(9) Information that is included in a limited data set as described by 45 C.F.R. 164.514(e), to the extent that the information is used,

LB1294
2024

disclosed, and maintained in the manner specified by 45 C.F.R. 164.514(e), as such regulation existed on January 1, 2024;

(10) Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act;

(11) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., as such act existed on January 1, 2024;

(12) Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as such act existed on January 1, 2024;

(13) Personal data regulated by the federal Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, as such act existed on January 1, 2024;

(14) Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act of 1971, 12 U.S.C. 2001 et seq., as such act existed on January 1, 2024;

(15) Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role;

(16) Data processed or maintained as the emergency contact information of an individual under the Data Privacy Act that is used for emergency contact purposes; or

(17) Data that is processed or maintained and is necessary to retain

LB1294
2024

to administer benefits for another individual that relates to an individual described by subdivision (15) of this section and used for the purposes of administering such benefits.

Sec. 5. The Data Privacy Act does not apply to the processing of personal data by a person in the course of a purely personal or household activity.

Sec. 6. A controller or processor that complies with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq., as such act existed on January 1, 2024, with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent under the Data Privacy Act.

Sec. 7. (1) A consumer may at any time submit a request to a controller specifying the consumer rights the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on behalf of the child.

(2) A controller shall comply with an authenticated consumer request to exercise the right to:

(a) Confirm whether a controller is processing the consumer's personal data and to access the personal data;

(b) Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(c) Delete personal data provided by or obtained about the consumer;

(d) If the data is available in a digital format, obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; or

(e) Opt out of the processing of the personal data for purposes of:

LB1294
2024

(i) Targeted advertising;

(ii) The sale of personal data; or

(iii) Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Sec. 8. (1) Except as otherwise provided in the Data Privacy Act, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to section 7 of this act.

(2) A controller shall respond to the consumer request within forty-five days after the date of receipt of the request. The controller may extend the response period once by an additional forty-five days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five-day response period, together with the reason for the extension.

(3) If a controller declines to comply with a consumer's request, the controller shall inform the consumer within forty-five days after the date of receipt of the request of the justification for declining to comply and provide instructions on how to appeal the decision to the Attorney General in accordance with section 9 of this act.

(4) A controller shall provide information in response to a consumer request free of charge, at least twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating that a request is manifestly unfounded, excessive, or repetitive.

(5) If a controller is unable to authenticate the request using commercially reasonable efforts, the controller is not required to comply with a consumer request submitted under section 7 of this act and may request that the consumer provide additional information reasonably

LB1294
2024

necessary to authenticate the consumer's identity and the consumer's request.

(6) A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete such personal data pursuant to subdivision (2)(c) of section 7 of this act by:

(a) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using the retained data for any other purpose under the Data Privacy Act; or

(b) Opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the Data Privacy Act.

Sec. 9. (1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under subsection (3) of section 8 of this act.

(2) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under section 7 of this act.

(3) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section not later than the sixtieth day after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

(4) If the controller denies an appeal, the controller shall provide the consumer with the online mechanism described by section 8 of this act through which the consumer may contact the Attorney General to submit a complaint.

Sec. 10. Any provision of a contract or agreement that waives or limits in any way a consumer right described in sections 7 to 9 of this act is contrary to public policy and is void and unenforceable.

LB1294
2024

Sec. 11. (1) A controller shall establish two or more secure and reliable methods to enable a consumer to submit a request to exercise consumer rights under the Data Privacy Act. The methods shall take into account:

(a) The ways in which consumers normally interact with the controller;

(b) The necessity for secure and reliable communications of those requests; and

(c) The ability of the controller to authenticate the identity of the consumer making the request.

(2) A controller shall not require a consumer to create a new account to exercise a consumer right under the Data Privacy Act, but may require a consumer to use an existing account.

(3) Except as provided by subsection (4) of this section, if the controller maintains an Internet website, the controller shall provide a mechanism on the website for a consumer to submit a request for information required to be disclosed under the Data Privacy Act.

(4) A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information is only required to provide an email address for the submission of a request described by subsection (3) of this section.

(5) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under subdivisions (2)(e)(i) and (ii) of section 7 of this act. A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller is able to verify, with commercially reasonable effort,

LB1294
2024

the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if:

(a) The authorized agent does not communicate the request to the controller in a clear and unambiguous manner;

(b) The controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state;

(c) The controller does not possess the ability to process the request; or

(d) The controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state.

(6) A technology described by subsection (5) of this section:

(a) Shall not unfairly disadvantage another controller;

(b) Shall not make use of a default setting, but shall require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data; and

(c) Shall be consumer-friendly and easy to use by the average consumer.

Sec. 12. (1) A controller:

(a) Shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer; and

(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue.

(2) A controller shall not:

LB1294
2024

(a) Except as otherwise provided in the Data Privacy Act, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

(b) Process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;

(c) Discriminate against a consumer for exercising any of the consumer rights contained in the Data Privacy Act, including by denying a good or service, charging a different price or rate for a good or service, or providing a different level of quality of a good or service to the consumer; or

(d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data in accordance with the federal Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq., as such act existed on January 1, 2024.

(3) Subdivision (2)(c) of this section shall not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee, if the consumer has exercised the consumer's right to opt out under section 7 of this act or the offer is related to a consumer's voluntary participation in a bona fide loyalty, reward, premium feature, discount, or club card program.

Sec. 13. (1) A controller shall provide each consumer with a reasonably accessible and clear privacy notice that includes:

(a) The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;

(b) The purpose for processing personal data;

LB1294
2024

(c) How a consumer may exercise a consumer right under sections 7 to 11 of this act, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request;

(d) If applicable, any category of personal data that the controller shares with any third party;

(e) If applicable, any category of third party with whom the controller shares personal data; and

(f) A description of each method required under section 11 of this act through which a consumer may submit a request to exercise a consumer right under the Data Privacy Act.

(2) If a controller engages in the sale of personal data that is sensitive data, the controller shall include the following notice posted in the same location and in the same manner as the privacy notice described by subsection (1) of this section:

NOTICE: We may sell your sensitive personal data.

(3) If a controller engages in the sale of personal data that is biometric data, the controller shall include the following notice posted in the same location and in the same manner as the privacy notice described by subsection (1) of this section:

NOTICE: We may sell your biometric personal data.

Sec. 14. If a controller sells personal data to any third party or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.

Sec. 15. (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties or requirements under the Data Privacy Act, including:

(a) Assisting the controller in responding to consumer rights requests submitted under section 7 of this act by using appropriate technical and organizational measures, as reasonably practicable, taking

LB1294
2024

into account the nature of processing and the information available to the processor;

(b) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system relating to an operator's or driver's license, taking into account the nature of processing and the information available to the processor; and

(c) Providing necessary information to enable the controller to conduct and document data protection assessments under section 16 of this act.

(2) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall include:

(a) Clear instructions for processing data;

(b) The nature and purpose of processing;

(c) The type of data subject to processing;

(d) The duration of processing;

(e) The rights and obligations of both parties; and

(f) A requirement that the processor shall:

(i) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(ii) At the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;

(iii) Make available to the controller, on reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the requirements of the Data Privacy Act;

(iv) Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and

(v) Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with

LB1294
2024

respect to the personal data.

(3) Notwithstanding the requirement described by subdivision (2)(f)(iv) of this section, a processor, in the alternative, may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under the Data Privacy Act using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller on request.

(4) This section shall not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of the role of the controller or processor in the processing relationship as described in the Data Privacy Act.

(5) A determination of whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Sec. 16. (1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising;

(b) The sale of personal data;

(c) The processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

(i) Unfair or deceptive treatment of or unlawful disparate impact on any consumer;

(ii) Financial, physical, or reputational injury to any consumer;

(iii) A physical or other intrusion on the solitude or seclusion, or

LB1294
2024

the private affairs or concerns, of any consumer, if the intrusion would be offensive to a reasonable person; or

(iv) Other substantial injury to any consumer;

(d) The processing of sensitive data; and

(e) Any processing activity that involves personal data that presents a heightened risk of harm to any consumer.

(2) A data protection assessment conducted under subsection (1) of this section shall:

(a) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks; and

(b) Factor into the assessment:

(i) The use of deidentified data;

(ii) The reasonable expectations of consumers;

(iii) The context of the processing; and

(iv) The relationship between the controller and the consumer whose personal data will be processed.

(3) A controller shall make a data protection assessment requested under subsection (2) of section 21 of this act available to the Attorney General pursuant to a civil investigative demand under section 21 of this act.

(4) A data protection assessment is confidential and exempt from disclosure as a public record pursuant to sections 84-712 to 84-712.09. Disclosure of a data protection assessment in compliance with a request from the Attorney General does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(5) A single data protection assessment may address a comparable set of processing operations that include similar activities.

LB1294
2024

(6) A data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

Sec. 17. (1) A controller in possession of deidentified data shall:

(a) Take reasonable measures to ensure that the data cannot be associated with an individual;

(b) Publicly commit to maintaining and using deidentified data without attempting to reidentify the data; and

(c) Contractually obligate any recipient of the deidentified data to comply with the Data Privacy Act.

(2) The Data Privacy Act shall not be construed to require a controller or processor to:

(a) Reidentify deidentified data or pseudonymous data;

(b) Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(c) Comply with an authenticated consumer rights request under section 7, if the controller:

(i) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

(iii) Does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted by this section.

(3) The consumer rights under subdivisions (2)(a) to (d) of section 7 of this act and controller duties under section 12 of this act do not

LB1294
2024

apply to pseudonymous data in any case in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(4) A controller that discloses pseudonymous data or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data is subject and shall take appropriate steps to address any breach of the contractual commitments.

Sec. 18. (1) A person described by subdivision (1)(c) of section 3 of this act shall not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer.

(2) A person who violates this section is subject to the penalty under section 24 of this act.

Sec. 19. The Attorney General has exclusive authority to enforce the Data Privacy Act.

Sec. 20. The Attorney General shall post on the Attorney General's website:

(1) Information relating to:

(a) The responsibilities of a controller under the Data Privacy Act;

(b) The responsibilities of a processor under the Data Privacy Act; and

(c) A consumer's rights under the Data Privacy Act; and

(2) An online mechanism through which a consumer may submit a complaint under the Data Privacy Act to the Attorney General.

Sec. 21. (1) If the Attorney General has reasonable cause to believe that a person has engaged in or is engaging in a violation of the Data Privacy Act, the Attorney General may issue a civil investigative demand pursuant to section 23 of this act.

(2) The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection

LB1294
2024

assessment that is relevant to an investigation conducted by the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with sections 12 to 14.

Sec. 22. Before bringing an action under section 24 of this act, the Attorney General shall notify a person in writing, not later than the thirtieth day before bringing the action, identifying the specific provisions of the Data Privacy Act the Attorney General alleges have been or are being violated. The Attorney General may not bring an action against the person if:

(1) Within the thirty-day period, the person cures the identified violation; and

(2) The person provides the Attorney General a written statement that the person:

(a) Cured the alleged violation;

(b) Notified the consumer that the consumer's privacy violation was addressed, if the consumer's contact information has been made available to the person;

(c) Provided supportive documentation to show how the privacy violation was cured; and

(d) Made changes to internal policies, if necessary, to ensure that no further violations will occur.

Sec. 23. (1) Whenever the Attorney General believes that any person may be in possession, custody, or control of any original or copy of any book, record, report, memorandum, paper, communication, tabulation, map, chart, photograph, mechanical transcription, or other tangible document or recording, wherever situated, which he or she believes to be relevant to the subject matter of an investigation of a possible violation of the Data Privacy Act, the Attorney General may, prior to the institution of a civil proceeding under such act, execute in writing and cause to be served upon such a person a civil investigative demand requiring such person to produce such documentary material and permit inspection and

LB1294
2024

copying thereof. This section shall not be applicable to criminal prosecutions.

(2) Each such demand shall:

(a) State the statute and section or sections thereof the alleged violation of which is under investigation, and the general subject matter of the investigation;

(b) Describe the class or classes of documentary material to be produced thereunder with reasonable specificity so as fairly to indicate the material demanded;

(c) Prescribe a return date within which the documentary material shall be produced; and

(d) Identify the members of the Attorney General's staff to whom such documentary material shall be made available for inspection and copying.

(3) No such demand shall:

(a) Contain any requirement which would be unreasonable or improper if contained in a subpoena duces tecum issued by a court of this state; or

(b) Require the disclosure of any documentary material which would be privileged, or which for any other reason would not be required by a subpoena duces tecum issued by a court of this state.

(4) Service of any such demand may be made by:

(a) Delivering a duly executed copy thereof to the person to be served, or, if such person is not a natural person, to any officer of the person to be served;

(b) Delivering a duly executed copy thereof to the principal place of business in this state of the person to be served; or

(c) Mailing by certified mail a duly executed copy thereof addressed to the person to be served at the principal place of business in this state, or, if such person has no place of business in this state, to his or her principal office or place of business.

LB1294
2024

(5) Documentary material demanded pursuant to the provisions of this section shall be produced for inspection and copying during normal business hours at the principal office or place of business of the person served, or at such other times and places as may be agreed upon by the person served and the Attorney General.

(6) No documentary material produced pursuant to a demand, or copies thereof, shall, unless otherwise ordered by a district court for good cause shown, be produced for inspection or copying by, nor shall the contents thereof be disclosed to, other than an authorized employee of the Attorney General, without the consent of the person who produced such material, except that:

(a) Under such reasonable terms and conditions as the Attorney General shall prescribe, the copies of such documentary material shall be available for inspection and copying by the person who produced such material or any duly authorized representative of such person;

(b) The Attorney General may provide copies of such documentary material to an official of this or any other state, or an official of the federal government, who is charged with the enforcement of federal or state antitrust or consumer protection laws, if such official agrees in writing to not disclose such documentary material to any person other than the official's authorized employees, except as such disclosure is permitted under subdivision (c) of this subsection; and

(c) The Attorney General or any assistant attorney general or an official authorized to receive copies of documentary material under subdivision (b) of this subsection may use such copies of documentary material as he or she determines necessary in the enforcement of the Data Privacy Act, including presentation before any court, except that any such material that contains trade secrets shall not be presented except with the approval of the court in which action is pending after adequate notice to the person furnishing such material.

(7) At any time before the return date specified in the demand, or

LB1294
2024

within twenty days after the demand has been served, whichever period is shorter, a petition to extend the return date for or to modify or set aside a demand issued pursuant to subsection (1) of this section, stating good cause, may be filed in the district court for Lancaster County, or in such other county where the parties reside. A petition by the person on whom the demand is served, stating good cause, to require the Attorney General or any person to perform any duty imposed by the provisions of this section, and all other petitions in connection with a demand, may be filed in the district court for Lancaster County or in the county where the parties reside.

(8) Whenever any person fails to comply with any civil investigative demand for documentary material duly served upon him or her under this section, or whenever satisfactory copying or reproduction of any such material cannot be done and such person refuses to surrender such material, the Attorney General may file, in the district court of the county in which such person resides, is found, or transacts business, and serve upon such person a petition for an order of such court for the enforcement of this section, except that if such person transacts business in more than one county such petition shall be filed in the county in which such person maintains his or her principal place of business or in such other county as may be agreed upon by the parties to such petition. Whenever any petition is filed in the district court of any county under this section, such court shall have jurisdiction to hear and determine the matter so presented and to enter such order as may be required to carry into effect the provisions of this section. Disobedience of any order entered under this section by any court shall be punished as a contempt thereof.

Sec. 24. (1) A person who violates the Data Privacy Act following the cure period described by section 22 of this act or who breaches a written statement provided to the Attorney General under that section is liable for a civil penalty in an amount not to exceed seven thousand five

LB1294
2024

hundred dollars for each violation.

(2) The Attorney General may bring an action in the name of the State of Nebraska to:

(a) Recover a civil penalty under this section;

(b) Restrain or enjoin the person from violating the Data Privacy Act; or

(c) Recover the civil penalty and seek injunctive relief.

(3) The Attorney General may recover reasonable attorney's fees and other reasonable expenses incurred in investigating and bringing an action under this section.

(4) All money collected under this section shall be remitted to the State Treasurer for distribution in accordance with Article VII, section 5, of the Constitution of Nebraska.

Sec. 25. The Data Privacy Act shall not be construed as providing a basis for, or being subject to, a private right of action for a violation of the Data Privacy Act or any other law.

Sec. 26. (1) The Data Privacy Act shall not be construed to restrict a controller's or processor's ability to:

(a) Comply with federal, state, or local laws, rules, or regulations;

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(c) Investigate, establish, exercise, prepare for, or defend legal claims;

(d) Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take action at the request of the consumer before entering into a contract;

(e) Take immediate action to protect an interest that is essential

LB1294
2024

for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;

(f) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(g) Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;

(h) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:

(i) If the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(ii) Whether the expected benefits of the research outweigh the privacy risks; and

(iii) If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

(i) Assist another controller, processor, or third party with any of the requirements under this subsection.

(2) The Data Privacy Act shall not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(3) The Data Privacy Act shall not be construed as imposing a requirement on any controller or processor that adversely affects any right or freedom of any person, including the right of free speech.

(4) The Data Privacy Act shall not be construed as requiring a controller, processor, third party, or consumer to disclose a trade

LB1294
2024

secret.

Sec. 27. (1) The requirements imposed on any controller or processor under the Data Privacy Act shall not restrict a controller's or processor's ability to collect, use, or retain data to:

(a) Conduct internal research to develop, improve, or repair products, services, or technology;

(b) Effect a product recall;

(c) Identify and repair technical errors that impair existing or intended functionality; or

(d) Perform internal operations that:

(i) Are reasonably aligned with the expectations of the consumer;

(ii) Are reasonably anticipated based on the consumer's existing relationship with the controller; or

(iii) Are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(2) A requirement imposed on a controller or processor under the Data Privacy Act shall not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under any law of this state.

Sec. 28. (1) A controller or processor that discloses personal data to a third-party controller or processor, in compliance with any requirement of the Data Privacy Act, does not violate the Data Privacy Act if the third-party controller or processor that receives and processes that personal data is in violation of the Data Privacy Act, if at the time of the data's disclosure the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(2) A third-party controller or processor that receives personal data from a controller or processor in compliance with the requirements

LB1294
2024

of the Data Privacy Act does not violate the Data Privacy Act for the transgressions of the controller or processor from which the third-party controller or processor received the personal data.

Sec. 29. (1) Personal data processed by a controller under this sections 26 to 29 of this act may not be processed for any purpose other than a purpose listed in sections 26 to 29 of this act unless otherwise allowed by the Data Privacy Act. Personal data processed by a controller under sections 26 to 29 of this act may be processed to the extent that the processing of the data is:

(a) Reasonably necessary and proportionate to the purposes listed in sections 26 to 29 of this act; and

(b) Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in sections 26 to 29 of this act.

(2) Personal data collected, used, or retained under subsection (1) of section 27 of this act shall, where applicable, take into account the nature and purpose of such collection, use, or retention. The personal data described by this subsection is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(3) A controller that processes personal data under an exemption in sections 26 to 29 of this act bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of subsections (1) and (2) of this section.

(4) The processing of personal data by an entity for the purposes described by section 26 of this act does not solely make the entity a controller with respect to the processing of the data.

Sec. 30. The Data Privacy Acct supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a political subdivision regarding the processing of personal data by a controller or

LB1294
2024

processor.

Sec. 31. Section 71-605.02, Reissue Revised Statutes of Nebraska, is amended to read:

71-605.02 The department shall preserve permanently ~~and index~~ all such certificates and shall charge and collect in advance the fee prescribed in section 71-612, to be paid by the applicant for each certified copy supplied to the applicant or for any search made at the applicant's request for access to or a certified copy of any record, whether or not the record is found on file with the department. All fees so collected shall be remitted to the State Treasurer for credit to the Health and Human Services Cash Fund as provided in section 71-612.

Sec. 32. Section 71-612, Revised Statutes Supplement, 2023, is amended to read:

71-612 (1) The department, as the State Registrar, shall preserve permanently ~~and index~~ all certificates received. The department shall supply to any applicant for any proper purpose, as defined by rules and regulations of the department, a certified copy of the record of any birth, death, marriage, annulment, or dissolution of marriage or an abstract of marriage. The department shall supply a copy of a public vital record for viewing purposes at its office upon an application signed by the applicant and upon proof of the identity of the applicant. The application may include the name, address, and telephone number of the applicant, purpose for viewing each record, and other information as may be prescribed by the department by rules and regulations to protect the integrity of vital records and prevent their fraudulent use. Except as provided in subsections (2), (3), (5), (6), (7), and (9) of this section, the department shall be entitled to charge and collect in advance a fee of sixteen dollars to be paid by the applicant for each certified copy or abstract of marriage supplied to the applicant or for any search made at the applicant's request for access to or a certified copy of any record or abstract of marriage, whether or not the record or

LB1294
2024

abstract is found on file with the department.

(2) The department shall, free of charge, search for and furnish a certified copy of any record or abstract of marriage on file with the department upon the request of (a) the United States Department of Veterans Affairs or any lawful service organization empowered to represent veterans if the copy of the record or abstract of marriage is to be issued, for the welfare of any member or veteran of the armed forces of the United States or in the interests of any member of his or her family, in connection with a claim growing out of service in the armed forces of the nation or (b) the Military Department.

(3) The department may, free of charge, search for and furnish a certified copy of any record or abstract of marriage on file with the department when in the opinion of the department it would be a hardship for the claimant of old age, survivors, or disability benefits under the federal Social Security Act to pay the fee provided in this section.

(4) A strict account shall be kept of all funds received by the department. Funds received pursuant to subsections (1), (5), (6), and (8) of this section shall be remitted to the State Treasurer for credit to the Health and Human Services Cash Fund. Money credited to the fund pursuant to this section shall be used for the purpose of administering the laws relating to vital statistics and may be used to create a petty cash fund administered by the department to facilitate the payment of refunds to individuals who apply for copies or abstracts of records. The petty cash fund shall be subject to section 81-104.01, except that the amount in the petty cash fund shall not be less than twenty-five dollars nor more than one thousand dollars.

(5) The department shall, upon request, conduct a search of death certificates for stated individuals for the Nebraska Medical Association or any of its allied medical societies or any inhospital staff committee pursuant to sections 71-3401 to 71-3403. If such death certificate is found, the department shall provide a noncertified copy. The department

LB1294
2024

shall charge a fee for each search or copy sufficient to cover its actual direct costs, except that the fee shall not exceed three dollars per individual search or copy requested.

(6) The department may permit use of data from vital records for statistical or research purposes under section 71-602 or disclose data from certificates or records to federal, state, county, or municipal agencies of government for use in administration of their official duties for the limited purposes of preventing, identifying, or halting fraudulent activity or waste of government funding. The department shall ~~and~~ charge and collect a fee that will recover the department's cost of production of the data. The department may provide access to public vital records for viewing purposes by electronic means, if available, under security provisions which shall assure the integrity and security of the records and database and shall charge and collect a fee that shall recover the department's costs.

(7) In addition to the fees charged under subsection (1) of this section, the department shall charge and collect an additional fee of one dollar for any certified copy of the record of any birth or for any search made at the applicant's request for access to or a certified copy of any such record, whether or not the record is found on file with the department. Any county containing a city of the metropolitan class which has an established city-county or county health department pursuant to sections 71-1626 to 71-1636 which has an established system of registering births and deaths shall charge and collect in advance a fee of one dollar for any certified copy of the record of any birth or for any search made at the applicant's request for such record, whether or not the record is found on file with the county. All fees collected under this subsection shall be remitted to the State Treasurer for credit to the Nebraska Child Abuse Prevention Fund.

(8) The department shall not charge other state agencies the fees authorized under subsections (1) and (7) of this section for automated

LB1294
2024

review of any certificates or abstracts of marriage. The department shall charge and collect a fee from other state agencies for such automated review that will recover the department's cost.

(9) The department shall not charge any fee for a certified copy of a birth record if the applicant does not have a current Nebraska driver's license or state identification card and indicates in the application that the applicant needs a certified copy of the birth record to apply for a state identification card for voting purposes.

Sec. 33. Section 71-616, Reissue Revised Statutes of Nebraska, is amended to read:

71-616 The department shall preserve permanently ~~and index~~ all births, deaths, marriages, and divorces received, and shall tabulate statistics therefrom.

Sec. 34. Section 84-712.05, Revised Statutes Cumulative Supplement, 2022, is amended to read:

84-712.05 The following records, unless publicly disclosed in an open court, open administrative proceeding, or open meeting or disclosed by a public entity pursuant to its duties, may be withheld from the public by the lawful custodian of the records:

(1) Personal information in records regarding a student, prospective student, or former student of any educational institution or exempt school that has effectuated an election not to meet state approval or accreditation requirements pursuant to section 79-1601 when such records are maintained by and in the possession of a public entity, other than routine directory information specified and made public consistent with 20 U.S.C. 1232g, as such section existed on February 1, 2013, and regulations adopted thereunder;

(2) Medical records, other than records of births and deaths and except as provided in subdivisions ~~subdivision~~ (5) and (26) of this section, in any form concerning any person; records of elections filed under section 44-2821; and patient safety work product under the Patient

LB1294
2024

Safety Improvement Act;

(3) Trade secrets, academic and scientific research work which is in progress and unpublished, and other proprietary or commercial information which if released would give advantage to business competitors and serve no public purpose;

(4) Records which represent the work product of an attorney and the public body involved which are related to preparation for litigation, labor negotiations, or claims made by or against the public body or which are confidential communications as defined in section 27-503;

(5) Records developed or received by law enforcement agencies and other public bodies charged with duties of investigation or examination of persons, institutions, or businesses, when the records constitute a part of the examination, investigation, intelligence information, citizen complaints or inquiries, informant identification, or strategic or tactical information used in law enforcement training, except that this subdivision shall not apply to records so developed or received:

(a) Relating to the presence of and amount or concentration of alcohol or drugs in any body fluid of any person; or

(b) Relating to the cause of or circumstances surrounding the death of an employee arising from or related to his or her employment if, after an investigation is concluded, a family member of the deceased employee makes a request for access to or copies of such records. This subdivision does not require access to or copies of informant identification, the names or identifying information of citizens making complaints or inquiries, other information which would compromise an ongoing criminal investigation, or information which may be withheld from the public under another provision of law. For purposes of this subdivision, family member means a spouse, child, parent, sibling, grandchild, or grandparent by blood, marriage, or adoption;

(6) The identity and personal identifying information of an alleged victim of sexual assault or sex trafficking as provided in section

LB1294
2024

29-4316;

(7) Appraisals or appraisal information and negotiation records concerning the purchase or sale, by a public body, of any interest in real or personal property, prior to completion of the purchase or sale;

(8) Personal information in records regarding personnel of public bodies other than salaries and routine directory information;

(9) Information solely pertaining to protection of the security of public property and persons on or within public property, such as specific, unique vulnerability assessments or specific, unique response plans, either of which is intended to prevent or mitigate criminal acts the public disclosure of which would create a substantial likelihood of endangering public safety or property; computer or communications network schema, passwords, and user identification names; guard schedules; lock combinations; or public utility infrastructure specifications or design drawings the public disclosure of which would create a substantial likelihood of endangering public safety or property, unless otherwise provided by state or federal law;

(10) Information that relates details of physical and cyber assets of critical energy infrastructure or critical electric infrastructure, including (a) specific engineering, vulnerability, or detailed design information about proposed or existing critical energy infrastructure or critical electric infrastructure that (i) relates details about the production, generation, transportation, transmission, or distribution of energy, (ii) could be useful to a person in planning an attack on such critical infrastructure, and (iii) does not simply give the general location of the critical infrastructure and (b) the identity of personnel whose primary job function makes such personnel responsible for (i) providing or granting individuals access to physical or cyber assets or (ii) operating and maintaining physical or cyber assets, if a reasonable person, knowledgeable of the electric utility or energy industry, would conclude that the public disclosure of such identity could create a

LB1294
2024

substantial likelihood of risk to such physical or cyber assets. Subdivision (10)(b) of this section shall not apply to the identity of a chief executive officer, general manager, vice president, or board member of a public entity that manages critical energy infrastructure or critical electric infrastructure. The lawful custodian of the records must provide a detailed job description for any personnel whose identity is withheld pursuant to subdivision (10)(b) of this section. For purposes of subdivision (10) of this section, critical energy infrastructure and critical electric infrastructure mean existing and proposed systems and assets, including a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of such matters;

(11) The security standards, procedures, policies, plans, specifications, diagrams, access lists, and other security-related records of the Lottery Division of the Department of Revenue and those persons or entities with which the division has entered into contractual relationships. Nothing in this subdivision shall allow the division to withhold from the public any information relating to amounts paid persons or entities with which the division has entered into contractual relationships, amounts of prizes paid, the name of the prize winner, and the city, village, or county where the prize winner resides;

(12) With respect to public utilities and except as provided in sections 43-512.06 and 70-101, personally identified private citizen account payment and customer use information, credit information on others supplied in confidence, and customer lists;

(13) Records or portions of records kept by a publicly funded library which, when examined with or without other records, reveal the identity of any library patron using the library's materials or services;

(14) Correspondence, memoranda, and records of telephone calls related to the performance of duties by a member of the Legislature in

LB1294
2024

whatever form. The lawful custodian of the correspondence, memoranda, and records of telephone calls, upon approval of the Executive Board of the Legislative Council, shall release the correspondence, memoranda, and records of telephone calls which are not designated as sensitive or confidential in nature to any person performing an audit of the Legislature. A member's correspondence, memoranda, and records of confidential telephone calls related to the performance of his or her legislative duties shall only be released to any other person with the explicit approval of the member;

(15) Records or portions of records kept by public bodies which would reveal the location, character, or ownership of any known archaeological, historical, or paleontological site in Nebraska when necessary to protect the site from a reasonably held fear of theft, vandalism, or trespass. This section shall not apply to the release of information for the purpose of scholarly research, examination by other public bodies for the protection of the resource or by recognized tribes, the Unmarked Human Burial Sites and Skeletal Remains Protection Act, or the federal Native American Graves Protection and Repatriation Act;

(16) Records or portions of records kept by public bodies which maintain collections of archaeological, historical, or paleontological significance which reveal the names and addresses of donors of such articles of archaeological, historical, or paleontological significance unless the donor approves disclosure, except as the records or portions thereof may be needed to carry out the purposes of the Unmarked Human Burial Sites and Skeletal Remains Protection Act or the federal Native American Graves Protection and Repatriation Act;

(17) Library, archive, and museum materials acquired from nongovernmental entities and preserved solely for reference, research, or exhibition purposes, for the duration specified in subdivision (17)(b) of this section, if:

(a) Such materials are received by the public custodian as a gift,

LB1294
2024

purchase, bequest, or transfer; and

(b) The donor, seller, testator, or transferor conditions such gift, purchase, bequest, or transfer on the materials being kept confidential for a specified period of time;

(18) Job application materials submitted by applicants, other than finalists or a priority candidate for a position described in section 85-106.06 selected using the enhanced public scrutiny process in section 85-106.06, who have applied for employment by any public body as defined in section 84-1409. For purposes of this subdivision, (a) job application materials means employment applications, resumes, reference letters, and school transcripts and (b) finalist means any applicant who is not an applicant for a position described in section 85-106.06 and (i) who reaches the final pool of applicants, numbering four or more, from which the successful applicant is to be selected, (ii) who is an original applicant when the final pool of applicants numbers less than four, or (iii) who is an original applicant and there are four or fewer original applicants;

(19)(a) Records obtained by the Public Employees Retirement Board pursuant to section 84-1512 and (b) records maintained by the board of education of a Class V school district and obtained by the board of trustees or the Public Employees Retirement Board for the administration of a retirement system provided for under the Class V School Employees Retirement Act pursuant to section 79-989;

(20) Social security numbers; credit card, charge card, or debit card numbers and expiration dates; and financial account numbers supplied to state and local governments by citizens;

(21) Information exchanged between a jurisdictional utility and city pursuant to section 66-1867;

(22) Draft records obtained by the Nebraska Retirement Systems Committee of the Legislature and the Governor from Nebraska Public Employees Retirement Systems pursuant to subsection (4) of section

LB1294
2024

84-1503;

(23) All prescription drug information submitted pursuant to section 71-2454, all data contained in the prescription drug monitoring system, and any report obtained from data contained in the prescription drug monitoring system;

(24) Information obtained by any government entity, whether federal, state, county, or local, regarding firearm registration, possession, sale, or use that is obtained for purposes of an application permitted or required by law or contained in a permit or license issued by such entity. Such information shall be available upon request to any federal, state, county, or local law enforcement agency; ~~and~~

(25) The security standards, procedures, policies, plans, specifications, diagrams, and access lists and other security-related records of the State Racing and Gaming Commission, those persons or entities with which the commission has entered into contractual relationships, and the names of any individuals placed on the list of self-excluded persons with the commission as provided in section 9-1118. Nothing in this subdivision shall allow the commission to withhold from the public any information relating to the amount paid any person or entity with which the commission has entered into a contractual relationship, the amount of any prize paid, the name of the prize winner, and the city, village, or county where the prize winner resides; ~~.~~

(26) Vital event records, unless all information designated as confidential under the Vital Statistics Act or all personally identifiable information is redacted by the Department of Health and Human Services;

(27) Information or records from historical indexes within one hundred years after the event date of the information or record; and

(28) The certificate number for any vital event certificate.

Sec. 35. This act becomes operative on January 1, 2025.

Sec. 36. If any section in this act or any part of any section is

LB1294
2024

declared invalid or unconstitutional, the declaration shall not affect the validity or constitutionality of the remaining portions.

Sec. 37. Original sections 71-605.02 and 71-616, Reissue Revised Statutes of Nebraska, section 84-712.05, Revised Statutes Cumulative Supplement, 2022, and section 71-612, Revised Statutes Supplement, 2023, are repealed.