

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:

1 A BILL FOR AN ACT relating to data privacy; to amend sections 71-605.02  
2 and 71-616, Reissue Revised Statutes of Nebraska, section 84-712.05,  
3 Revised Statutes Cumulative Supplement, 2022, and section 71-612,  
4 Revised Statutes Supplement, 2023; to adopt the Data Privacy Act; to  
5 change provisions relating to the preservation and use of certain  
6 certificates and information relating to vital records; to provide  
7 for certain records to be exempt from public disclosure; to provide  
8 an operative date; to provide severability; and to repeal the  
9 original sections.  
10 Be it enacted by the people of the State of Nebraska,

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

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

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

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

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

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

14          (2) Authenticate means to verify through reasonable means that the  
15 consumer who is entitled to exercise the consumer's rights under sections  
16 7 to 11 of this act is the same consumer exercising those consumer rights  
17 with respect to the personal data at issue;

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

21           (i) Fingerprint;

22           (ii) Voice print;

23           (iii) Retina image;

24           (iv) Iris image;

25           (v) Information derived from wastewater; or

26           (vi) Unique biological pattern or characteristic; and

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

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

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

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

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

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

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

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

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

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

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

23       (9) Covered entity has the same meaning as defined in 45 C.F.R.  
24 160.103, as such regulation existed on January 1, 2024;

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

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

1        (a) Financial and lending services;

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

3        (c) Education enrollment;

4        (d) Employment opportunities;

5        (e) Criminal justice; or

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

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

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

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

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

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

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

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

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

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

1 age;

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

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

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

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

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

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

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

1 radius of one thousand seven hundred fifty feet.

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

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

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

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

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

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

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

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

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

3 (b) Sale of personal data does not include:

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

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

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

10 (iv) The disclosure of information that the consumer:

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

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

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

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

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

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

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

23 (d) Precise geolocation data;

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

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

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

2 (b) Targeted advertising does not include:

3 (i) An advertisement that:

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

18           (d) Nonprofit organization;

19           (e) Institution of higher education;

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

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

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

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

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

28           (2) Health records;

29           (3) Patient identifying information for purposes of 42 U.S.C.  
30 290dd-2, as such section existed on January 1, 2024;

31           (4) Identifiable private information:

1        (a) For purposes of the federal policy for the protection of human  
2 subjects under 45 C.F.R. part 46, as such part existed on January 1,  
3 2024;

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

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

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

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

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

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

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

1 disclosed, and maintained in the manner specified by 45 C.F.R.  
2 164.514(e), as such regulation existed on January 1, 2024;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 1        (i) Targeted advertising;
- 2        (ii) The sale of personal data; or
- 3        (iii) Profiling in furtherance of a decision that produces a legal
- 4 or similarly significant effect concerning the consumer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 (a) Shall not unfairly disadvantage another controller;

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

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

22 Sec. 12. (1) A controller:

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

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

31 (2) A controller shall not:



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

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

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

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

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

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

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

31        (b) The purpose for processing personal data;

1       (c) How a consumer may exercise a consumer right under sections 7 to  
2 11 of this act, including the process by which a consumer may appeal a  
3 controller's decision with regard to the consumer's request;

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

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

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

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

15       NOTICE: We may sell your sensitive personal data.

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

20       NOTICE: We may sell your biometric personal data.

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

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

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

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

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

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

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

14 (a) Clear instructions for processing data;

15 (b) The nature and purpose of processing;

16 (c) The type of data subject to processing;

17 (d) The duration of processing;

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

19 (f) A requirement that the processor shall:

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

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

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

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

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

1 respect to the personal data.

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

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

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

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

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

25 (b) The sale of personal data;

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

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

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

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

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

3 (iv) Other substantial injury to any consumer;

4 (d) The processing of sensitive data; and

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

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

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

14 (b) Factor into the assessment:

15 (i) The use of deidentified data;

16 (ii) The reasonable expectations of consumers;

17 (iii) The context of the processing; and

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

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

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

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

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

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

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

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

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

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

14       (a) Reidentify deidentified data or pseudonymous data;

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

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

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

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

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

30       (3) The consumer rights under subdivisions (2)(a) to (d) of section  
31 7 of this act and controller duties under section 12 of this act do not

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

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

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

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

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

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

19 (1) Information relating to:

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

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

22 and

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

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

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

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

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

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

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

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

14       (a) Cured the alleged violation;

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

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

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

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



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

3 (2) Each such demand shall:

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

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

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

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

15 (3) No such demand shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 hundred dollars for each violation.

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

4 (a) Recover a civil penalty under this section;

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

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

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

11 (4) All money collected under this section shall be remitted to the  
12 State Treasurer for distribution in accordance with Article VII, section  
13 5, of the Constitution of Nebraska.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 secret.

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

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

7 (b) Effect a product recall;

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

10 (d) Perform internal operations that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 processor.

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

4       71-605.02 The department shall preserve permanently ~~and index~~ all  
5 such certificates and shall charge and collect in advance the fee  
6 prescribed in section 71-612, to be paid by the applicant for each  
7 certified copy supplied to the applicant or for any search made at the  
8 applicant's request for access to or a certified copy of any record,  
9 whether or not the record is found on file with the department. All fees  
10 so collected shall be remitted to the State Treasurer for credit to the  
11 Health and Human Services Cash Fund as provided in section 71-612.

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

14       71-612 (1) The department, as the State Registrar, shall preserve  
15 permanently ~~and index~~ all certificates received. The department shall  
16 supply to any applicant for any proper purpose, as defined by rules and  
17 regulations of the department, a certified copy of the record of any  
18 birth, death, marriage, annulment, or dissolution of marriage or an  
19 abstract of marriage. The department shall supply a copy of a public  
20 vital record for viewing purposes at its office upon an application  
21 signed by the applicant and upon proof of the identity of the applicant.  
22 The application may include the name, address, and telephone number of  
23 the applicant, purpose for viewing each record, and other information as  
24 may be prescribed by the department by rules and regulations to protect  
25 the integrity of vital records and prevent their fraudulent use. Except  
26 as provided in subsections (2), (3), (5), (6), (7), and (9) of this  
27 section, the department shall be entitled to charge and collect in  
28 advance a fee of sixteen dollars to be paid by the applicant for each  
29 certified copy or abstract of marriage supplied to the applicant or for  
30 any search made at the applicant's request for access to or a certified  
31 copy of any record or abstract of marriage, whether or not the record or



1 abstract is found on file with the department.

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

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

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

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

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

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

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

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

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

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

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

11 71-616 The department shall preserve permanently ~~and index~~ all  
12 births, deaths, marriages, and divorces received, and shall tabulate  
13 statistics therefrom.

14 Sec. 34. Section 84-712.05, Revised Statutes Cumulative Supplement,  
15 2022, is amended to read:

16 84-712.05 The following records, unless publicly disclosed in an  
17 open court, open administrative proceeding, or open meeting or disclosed  
18 by a public entity pursuant to its duties, may be withheld from the  
19 public by the lawful custodian of the records:

20 (1) Personal information in records regarding a student, prospective  
21 student, or former student of any educational institution or exempt  
22 school that has effectuated an election not to meet state approval or  
23 accreditation requirements pursuant to section 79-1601 when such records  
24 are maintained by and in the possession of a public entity, other than  
25 routine directory information specified and made public consistent with  
26 20 U.S.C. 1232g, as such section existed on February 1, 2013, and  
27 regulations adopted thereunder;

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

1 Safety Improvement Act;

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

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

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

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

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

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

1 29-4316;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 purchase, bequest, or transfer; and

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

5 (18) Job application materials submitted by applicants, other than  
6 finalists or a priority candidate for a position described in section  
7 85-106.06 selected using the enhanced public scrutiny process in section  
8 85-106.06, who have applied for employment by any public body as defined  
9 in section 84-1409. For purposes of this subdivision, (a) job application  
10 materials means employment applications, resumes, reference letters, and  
11 school transcripts and (b) finalist means any applicant who is not an  
12 applicant for a position described in section 85-106.06 and (i) who  
13 reaches the final pool of applicants, numbering four or more, from which  
14 the successful applicant is to be selected, (ii) who is an original  
15 applicant when the final pool of applicants numbers less than four, or  
16 (iii) who is an original applicant and there are four or fewer original  
17 applicants;

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

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

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

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



1 84-1503;

2 (23) All prescription drug information submitted pursuant to section  
3 71-2454, all data contained in the prescription drug monitoring system,  
4 and any report obtained from data contained in the prescription drug  
5 monitoring system;

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

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

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

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

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

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

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

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

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