

HOUSE BILL 214

**57TH LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2026**

INTRODUCED BY

Linda Serrato and Joshua N. Hernandez and Anita Gonzales  
and Doreen Y. Gallegos

AN ACT

RELATING TO DATA; ENACTING THE CONSUMER INFORMATION AND DATA  
PROTECTION ACT; PROVIDING PROCESSES FOR THE COLLECTION AND  
PROTECTION OF DATA; PROVIDING DUTIES; PROVIDING EXCEPTIONS;  
PROVIDING INVESTIGATIVE AUTHORITY; PROVIDING CIVIL PENALTIES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be  
cited as the "Consumer Information and Data Protection Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the  
Consumer Information and Data Protection Act:

A. "affiliate" means a legal entity that shares  
common branding with another legal entity or controls, is  
controlled by or is under common control with another legal  
entity, including:

(1) ownership of, or the power to control the

1 vote of, more than fifty percent of the outstanding shares of a  
2 class of voting security of a company;

3 (2) control in any manner over the election of  
4 a majority of the directors or of individuals exercising  
5 similar functions; or

6 (3) the power to exercise controlling  
7 influence over the management of a company;

8 B. "authenticate" means to use reasonable means to  
9 determine that a request to exercise any of the rights afforded  
10 under Section 4 of the Consumer Information and Data Protection  
11 Act is being made by, or on behalf of, the consumer who is  
12 entitled to exercise those consumer rights with respect to the  
13 personal data at issue;

14 C. "biometric data" means data generated by  
15 automatic measurements of an individual's biological  
16 characteristics, such as a fingerprint, a voiceprint, eye  
17 retinas, irises or other unique biological patterns or  
18 characteristics that are used to identify a specific  
19 individual. "Biometric data" does not include:

20 (1) a digital or physical photograph;

21 (2) an audio or a video recording; or

22 (3) data generated from a digital or physical  
23 photograph or an audio or a video recording unless those data  
24 are generated to identify a specific individual;

25 D. "business associate" has the same meaning as

1 provided in the federal Health Insurance Portability and  
2 Accountability Act of 1996;

3 E. "child" means a person under the age of  
4 thirteen;

5 F. "consent" means a clear affirmative act  
6 signifying a consumer's freely given, specific, informed and  
7 unambiguous agreement to allow the processing of personal data  
8 relating to the consumer. "Consent" may include a written  
9 statement, including by electronic means, or other unambiguous  
10 affirmative action. "Consent" does not include:

11 (1) acceptance of a general or broad terms of  
12 use or similar document that contains descriptions of personal  
13 data processing along with other, unrelated information;

14 (2) hovering over, muting, pausing or closing  
15 a given piece of content; or

16 (3) agreement obtained through the use of dark  
17 patterns;

18 G. "consumer" means an individual who is a resident  
19 of this state. "Consumer" does not include an individual  
20 acting in a commercial or employment context or as an employee,  
21 an owner, a director, an officer or a contractor of a company,  
22 partnership, sole proprietorship, nonprofit organization or  
23 government agency whose communications or transactions with the  
24 controller occur solely within the context of that individual's  
25 role with the company, partnership, sole proprietorship,

.232991.lms

1 nonprofit organization or government agency;

2 H. "consumer health data" means personal data that  
3 a controller uses to identify a consumer's physical or mental  
4 health condition or diagnosis and includes gender-affirming  
5 health data and reproductive or sexual health data;

6 I. "controller" means a person who, alone or  
7 jointly with others, determines the purpose and means of  
8 processing personal data;

9 J. "covered entity" has the same meaning as  
10 provided in the federal Health Insurance Portability and  
11 Accountability Act of 1996;

12 K. "covered resident" means a natural person who  
13 lives in or is domiciled in New Mexico;

14 L. "dark pattern" means a user interface designed  
15 or manipulated with the substantial effect of subverting or  
16 impairing user autonomy, decision making or choice and includes  
17 any practice the federal trade commission refers to as a "dark  
18 pattern";

19 M. "decisions that produce legal or similarly  
20 significant effects concerning the consumer" means decisions  
21 made by a controller that result in the provision or denial by  
22 the controller of financial or lending services, housing,  
23 insurance, education enrollment or opportunity, criminal  
24 justice, employment opportunities, health care services or  
25 access to essential goods or services;

.232991.lms

1           N. "de-identified data" means data that cannot  
2 reasonably be used to infer information about, or otherwise be  
3 linked to, an identified or identifiable individual, or a  
4 device linked to the individual, if a controller that possesses  
5 the data:

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

8                   (2) publicly commits to processing the data  
9 only in a de-identified fashion and not attempting to re-  
10 identify the data; and

11                   (3) contractually obligates recipients of the  
12 data to satisfy the criteria set forth in Paragraphs (1) and  
13 (2) of this subsection;

14           O. "geofence" means technology that uses global  
15 positioning coordinates, cell tower connectivity, cellular  
16 data, radio frequency identification, wireless fidelity  
17 technology data or another form of location detection, or a  
18 combination of coordinates, connectivity, data, identification  
19 or other form of location detection, to establish a virtual  
20 boundary;

21           P. "heightened risk of harm to minors" means  
22 processing minors' personal data in a manner that presents a  
23 reasonably foreseeable risk of:

24                   (1) unfair or deceptive treatment of, or  
25 unlawful disparate impact on, minors;

.232991.lms

1 (2) financial, physical or reputational injury  
2 to minors; or

3 (3) physical or other intrusion upon the  
4 solitude or seclusion, or the private affairs or concerns, of  
5 minors if the intrusion would be offensive to a reasonable  
6 person;

7 Q. "identified or identifiable individual" means an  
8 individual who can be readily identified, directly or  
9 indirectly;

10 R. "institution of higher education" means a  
11 school, a board, an association, a limited liability company or  
12 a corporation that is licensed or accredited to offer one or  
13 more programs of higher learning leading to one or more  
14 degrees;

15 S. "mental health facility" means a health care  
16 facility at which at least seventy percent of the health care  
17 services provided are mental health services;

18 T. "online service, product or feature" means a  
19 service, product or feature that is provided online. "Online  
20 service, product or feature" does not include a:

21 (1) telecommunications service, as defined in  
22 47 U.S.C. I 53;

23 (2) broadband internet access service, as  
24 defined in 47 C.F.R. 54.400; or

25 (3) delivery or use of a physical product;

.232991.lms

1           U. "person" means an individual, an association, a  
2 company, a limited liability company, a corporation, a  
3 partnership, a sole proprietorship, a trust or other legal  
4 entity;

5           V. "personal data" means information that is linked  
6 or reasonably linkable to an identified or identifiable  
7 individual. "Personal data" does not include de-identified  
8 data or publicly available information;

9           W. "precise geolocation data" means information  
10 derived from technology, including global positioning system  
11 level latitude and longitude coordinates or other mechanisms,  
12 that directly identifies the specific location of an individual  
13 with precision and accuracy within a radius of one thousand  
14 seven hundred fifty feet. "Precise geolocation data" does not  
15 include the content of communications or data generated by or  
16 connected to advanced utility metering infrastructure systems  
17 or equipment for use by a utility;

18           X. "process" means an operation or set of  
19 operations performed, whether by manual or automated means, on  
20 personal data or on sets of personal data, such as the  
21 collection, use, storage, disclosure, analysis, deletion or  
22 modification of personal data;

23           Y. "processor" means a person that processes  
24 personal data on behalf of a controller;

25           Z. "profiling" means a form of automated processing

1 performed on personal data to evaluate, analyze or predict  
2 personal aspects related to an identified or identifiable  
3 individual's economic situation, health, personal preferences,  
4 interests, reliability, behavior, location or movements;

5 AA. "protected health information" has the same  
6 meaning as provided in the federal Health Insurance Portability  
7 and Accountability Act of 1996;

8 BB. "pseudonymous data" means personal data that  
9 cannot be attributed to a specific individual without the use  
10 of additional information; provided that the additional  
11 information is kept separately and is subject to appropriate  
12 technical and organizational measures to ensure that the  
13 personal data are not attributed to an identified or  
14 identifiable individual;

15 CC. "publicly available information" means  
16 information that:

17 (1) is lawfully made available through  
18 federal, state or local government records; and

19 (2) a person has a reasonable basis to believe  
20 a consumer has lawfully made available to the general public  
21 through widely distributed media, by the consumer or by a  
22 person to whom the consumer has disclosed the information,  
23 unless the consumer has restricted the information to a  
24 specific audience;

25 DD. "reproductive or sexual health care" means



1 health care-related services or products rendered or provided  
2 concerning a consumer's reproductive system or sexual well-  
3 being, including a service or product rendered or provided  
4 concerning:

5 (1) an individual health condition, status,  
6 disease, diagnosis, diagnostic test or treatment;

7 (2) a social, psychological, behavioral or  
8 medical intervention;

9 (3) a surgery or procedure, including an  
10 abortion;

11 (4) a use or purchase of a medication,  
12 including a medication used or purchased for the purposes of an  
13 abortion;

14 (5) a bodily function, vital sign or symptom;

15 (6) a measurement of a bodily function, vital  
16 sign or symptom; or

17 (7) an abortion, including medical or  
18 nonmedical services, products, diagnostics, counseling or  
19 follow-up services for an abortion;

20 EE. "reproductive or sexual health facility" means  
21 a health care facility at which at least seventy percent of the  
22 health care-related services or products rendered or provided  
23 are reproductive or sexual health care;

24 FF. "sale of personal data" means the exchange of  
25 personal data for monetary or other valuable consideration by a

1 controller to a third party. "Sale of personal data" does not  
2 include:

3 (1) the disclosure of personal data to a  
4 processor that processes the personal data on behalf of the  
5 controller;

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

9 (3) the disclosure or transfer of personal  
10 data to an affiliate of the controller;

11 (4) the disclosure of personal data where the  
12 consumer directs the controller to disclose the personal data  
13 or intentionally uses the controller to interact with a third  
14 party;

15 (5) the disclosure of personal data that the  
16 consumer intentionally made available to the general public via  
17 a channel of mass media and did not restrict to a specific  
18 audience; or

19 (6) the disclosure or transfer of personal  
20 data to a third party as an asset that is part of a merger, an  
21 acquisition, a bankruptcy or other transaction, or a proposed  
22 merger, acquisition, bankruptcy or other transaction, in which  
23 the third party assumes control of all or part of the  
24 controller's assets;

25 GG. "sensitive data" means personal data that

.232991.lms

1 include:

2 (1) data revealing racial or ethnic origin,  
3 religious beliefs, a mental or physical health condition or  
4 diagnosis, information regarding a person's sex life, sexual  
5 orientation or citizenship or immigration status;

6 (2) consumer health data;

7 (3) the processing of genetic or biometric  
8 data for the purpose of uniquely identifying an individual;

9 (4) an individual's social security, driver's  
10 license, state identification card or passport number;

11 (5) an individual's account login, financial  
12 account, debit card or credit card number in combination with a  
13 required security or access code, password or credentials  
14 allowing access to an account;

15 (6) personal data collected from a child;

16 (7) data concerning an individual's status as  
17 a victim of crime; or

18 (8) precise geolocation data; and

19 HH. "targeted advertising" means displaying  
20 advertisements to a consumer where the advertisement is  
21 selected based on personal data obtained or inferred from that  
22 consumer's activities over time and across nonaffiliated  
23 websites or online applications to predict that consumer's  
24 preferences or interests. "Targeted advertising" does not  
25 include:

.232991.lms

1 (1) advertisements based on activities within  
2 a controller's own website or online applications;

3 (2) advertisements based on the context of a  
4 consumer's current search query, visit to a website or online  
5 application;

6 (3) advertisements directed to a consumer in  
7 response to the consumer's request for information or feedback;  
8 or

9 (4) processing personal data solely to measure  
10 or report advertising frequency, performance or reach.

11 SECTION 3. [NEW MATERIAL] SCOPE OF ACT--EXEMPTIONS.--

12 A. The Consumer Information and Data Protection Act  
13 applies to persons that conduct business in New Mexico and  
14 persons that produce products or services that are targeted to  
15 residents of New Mexico and that during the preceding calendar  
16 year did any of the following:

17 (1) controlled or processed the personal data  
18 of at least thirty-five thousand consumers, excluding personal  
19 data controlled or processed solely for the purpose of  
20 completing a payment transaction; or

21 (2) controlled or processed the personal data  
22 of at least ten thousand consumers and derived more than twenty  
23 percent of its gross revenue from the sale of personal data.

24 B. A person shall not:

25 (1) provide an employee or a contractor with

1 access to consumer health data unless the employee or  
2 contractor is subject to a contractual or statutory duty of  
3 confidentiality;

4 (2) provide a processor with access to  
5 consumer health data unless the person and processor comply  
6 with Section 9 of the Consumer Information and Data Protection  
7 Act;

8 (3) use a geofence to establish a virtual  
9 boundary that is within one thousand seven hundred fifty feet  
10 of a mental health facility or reproductive or sexual health  
11 facility for the purpose of identifying, tracking, collecting  
12 personal data from or sending any notification to a consumer  
13 regarding the consumer's consumer health data; or

14 (4) sell, or offer to sell, consumer health  
15 data without first obtaining the consumer's consent.

16 C. The provisions of the Consumer Information and  
17 Data Protection Act shall not apply to any:

18 (1) body, authority, board, bureau,  
19 commission, district or agency of the state or of any political  
20 subdivision of the state;

21 (2) financial institution or data subject to  
22 Title 5 of the federal Gramm-Leach-Bliley Act, 15 U.S.C.  
23 Sections 6801 through 6809;

24 (3) covered entity or business associate  
25 governed by the privacy, security and breach notification rules

.232991.lms

1 issued by the United States department of health and human  
2 services, 45 C.F.R. Parts 160 and 164 established pursuant to  
3 the federal Health Insurance Portability and Accountability Act  
4 of 1996, and the federal Health Information Technology for  
5 Economic and Clinical Health Act;

6 (4) nonprofit organization;

7 (5) institution of higher education;

8 (6) protected health information under the  
9 federal Health Insurance Portability and Accountability Act of  
10 1996;

11 (7) patient-identifying information for  
12 purposes of 42 U.S.C. Section 290dd-2;

13 (8) identifiable private information for  
14 purposes of the federal policy for the protection of human  
15 subjects under 45 C.F.R. Part 46; identifiable private  
16 information that is otherwise information collected as part of  
17 human subjects research pursuant to the good clinical practice  
18 guidelines issued by the international council for  
19 harmonization of technical requirements for pharmaceuticals for  
20 human use; the protection of human subjects under 21 C.F.R.  
21 Parts 6, 50 and 56; or personal data used or shared in research  
22 conducted in accordance with the requirements set forth in the  
23 Consumer Information and Data Protection Act or other research  
24 conducted in accordance with applicable law;

25 (9) information and documents created for

.232991.lms

1 purposes of the federal Health Care Quality Improvement Act of  
2 1986;

3 (10) patient safety work product for purposes  
4 of the federal Patient Safety and Quality Improvement Act of  
5 2005;

6 (11) information derived from the health  
7 care-related information listed in this subsection that is de-  
8 identified in accordance with the requirements for de-  
9 identification pursuant to the federal Health Insurance  
10 Portability and Accountability Act of 1996;

11 (12) information originating from, and  
12 intermingled to be indistinguishable with, or treated in the  
13 same manner as information exempt under this subsection that is  
14 maintained by a covered entity or business associate as defined  
15 by the federal Health Insurance Portability and Accountability  
16 Act of 1996 or a program or qualified service organization as  
17 defined by 42 U.S.C. Section 290dd-2;

18 (13) information used only for public health  
19 activities and purposes as authorized by the federal Health  
20 Insurance Portability and Accountability Act of 1996;

21 (14) collection, maintenance, disclosure,  
22 sale, communication or use of any personal information bearing  
23 on a consumer's creditworthiness, credit standing, credit  
24 capacity, character, general reputation, personal  
25 characteristics or mode of living by a consumer reporting

.232991.lms

1 agency or furnisher that provides information for use in a  
2 consumer report and by a user of a consumer report but only to  
3 the extent that the activity is regulated by and authorized  
4 under the federal Fair Credit Reporting Act;

5 (15) personal data collected, processed, sold  
6 or disclosed in compliance with the federal Driver's Privacy  
7 Protection Act of 1994;

8 (16) personal data regulated by the federal  
9 Family Educational Rights and Privacy Act of 1974;

10 (17) personal data collected, processed, sold  
11 or disclosed in compliance with the federal Farm Credit Act of  
12 1971; or

13 (18) personal data processed or maintained:

14 (a) in the course of an individual  
15 applying to, employed by or acting as an agent or independent  
16 contractor of a controller, processor or third party, to the  
17 extent that the personal data are collected and used within the  
18 context of that role;

19 (b) as the emergency contact information  
20 of an individual under the Consumer Information and Data  
21 Protection Act used for emergency contact purposes; or

22 (c) that is necessary to retain to  
23 administer benefits for another individual relating to the  
24 individual under Subparagraph (a) of this paragraph and used  
25 for the purposes of administering those benefits.

.232991.lms



1           SECTION 4.   ~~[NEW MATERIAL]~~ CONSUMER RIGHTS.--

2           A. A consumer may invoke the consumer rights  
3 pursuant to this section at any time by submitting a request to  
4 a controller specifying the consumer rights the consumer wishes  
5 to invoke. A child's parent or legal guardian may invoke  
6 consumer rights on behalf of the child regarding processing  
7 personal data belonging to the child. A controller shall  
8 comply with an authentic consumer request to exercise the right  
9 to:

10                       (1) confirm whether or not a controller is  
11 processing the consumer's personal data and to access the  
12 personal data;

13                       (2) correct inaccuracies in the consumer's  
14 personal data, taking into account the nature of the personal  
15 data and the purposes of the processing of the consumer's  
16 personal data;

17                       (3) delete personal data provided by or  
18 obtained about the consumer;

19                       (4) obtain a copy of the consumer's personal  
20 data that the consumer previously provided to the controller in  
21 a portable and, to the extent technically feasible, readily  
22 usable format that allows the consumer to transmit the data to  
23 another controller without hindrance, where the processing is  
24 carried out by automated means; and

25                       (5) opt out of the processing of the personal

.232991.lms

1 data for purposes of targeted advertising, the sale of personal  
2 data or profiling in furtherance of decisions that produce  
3 legal or similarly significant effects concerning the consumer.

4 B. A consumer may exercise rights under this  
5 section by a secure and reliable means established by the  
6 controller and described to the consumer in the controller's  
7 privacy notice. In the case of processing personal data of a  
8 child, the parent or legal guardian may exercise the consumer  
9 rights on the child's behalf. In the case of processing  
10 personal data concerning a consumer subject to a guardianship,  
11 conservatorship or other protective arrangement, the guardian  
12 or the conservator of the consumer may exercise the rights on  
13 the consumer's behalf.

14 C. Except as otherwise provided in the Consumer  
15 Information and Data Protection Act, a controller shall comply  
16 with a request by a consumer to exercise the consumer rights  
17 authorized pursuant to Subsection A of this section as follows:

18 (1) a controller shall respond to the consumer  
19 without undue delay, but no later than forty-five days after  
20 receipt of the request submitted pursuant to the methods  
21 described in Subsection A of this section. The response period  
22 may be extended once by forty-five additional days when  
23 reasonably necessary, taking into account the complexity and  
24 number of the consumer's requests, so long as the controller  
25 informs the consumer of any the extension within the initial

1 forty-five-day response period, including the reason for the  
2 extension;

3 (2) if a controller declines to take action  
4 regarding the consumer's request, the controller shall inform  
5 the consumer without undue delay, but no later than forty-five  
6 days after receipt of the request, of the justification for  
7 declining to take action and instructions for how to appeal the  
8 decision pursuant to Subsection D of this section;

9 (3) information provided in response to a  
10 consumer request shall be provided by a controller free of  
11 charge, up to twice annually per consumer. If requests from a  
12 consumer are manifestly unfounded, excessive or repetitive, the  
13 controller may charge the consumer a reasonable fee to cover  
14 the administrative costs of complying with the request or  
15 decline to act on the request. The controller bears the burden  
16 of demonstrating the manifestly unfounded, excessive or  
17 repetitive nature of the request;

18 (4) if a controller is unable to authenticate  
19 the request using commercially reasonable efforts, the  
20 controller shall not be required to comply with a request to  
21 initiate an action under Subsection A of this section and may  
22 request that the consumer provide additional information  
23 reasonably necessary to authenticate the consumer and the  
24 consumer's request;

25 (5) a controller that has obtained personal

.232991.lms

1 data about a consumer from a source other than the consumer  
2 shall be deemed in compliance with a consumer's request to  
3 delete personal data pursuant to Paragraph (2) of Subsection A  
4 of this section by either:

5 (a) retaining a record of the deletion  
6 request and the minimum data necessary for the purpose of  
7 ensuring the consumer's personal data remain deleted from the  
8 controller's records and not using the retained data for any  
9 other purpose pursuant to the provisions of the Consumer  
10 Information and Data Protection Act; or

11 (b) opting the consumer out of the  
12 processing of the personal data for any purpose except for  
13 those exempted pursuant to the provisions of the Consumer  
14 Information and Data Protection Act; and

15 (6) a controller shall provide an effective  
16 mechanism for a consumer to revoke the consumer's consent under  
17 this section that is at least as easy as the mechanism by which  
18 the consumer provided the consumer's consent and, upon  
19 revocation of consent, cease to process the data as soon as  
20 practicable, but no later than fifteen days after the receipt  
21 of the request.

22 D. A controller shall establish a process for a  
23 consumer to appeal the controller's refusal to take action on a  
24 request within a reasonable period of time after the consumer's  
25 receipt of the decision pursuant to Paragraph (2) of Subsection

1 C of this section. The appeal process shall be conspicuously  
2 available and similar to the process for submitting requests to  
3 initiate action pursuant to Subsection A of this section.

4 Within sixty days of receipt of an appeal, a controller shall  
5 inform the consumer in writing of any action taken or not taken  
6 in response to the appeal, including a written explanation of  
7 the reasons for the decisions. If the appeal is denied, the  
8 controller shall also provide the consumer with an online  
9 mechanism, if available, or other method through which the  
10 consumer may contact the attorney general to submit a  
11 complaint.

12 SECTION 5. [NEW MATERIAL] AUTHORIZED AGENTS AND CONSUMER  
13 OPT-OUT.--A consumer may designate another person to serve as  
14 the consumer's authorized agent, and act on the consumer's  
15 behalf, to opt out of the processing of the consumer's personal  
16 data for one or more of the purposes specified in Section 4 of  
17 the Consumer Information and Data Protection Act. The consumer  
18 may designate the authorized agent by way of a technology,  
19 including an internet link or a browser setting, browser  
20 extension or global device setting, indicating the consumer's  
21 intent to opt out of such processing. A controller shall  
22 comply with an opt-out request received from an authorized  
23 agent if the controller is able to verify, with commercially  
24 reasonable effort, the identity of the consumer and the  
25 authorized agent's authority to act on the consumer's behalf.

.232991.lms

1           SECTION 6.   [NEW MATERIAL] DATA CONTROLLER

2   RESPONSIBILITIES--TRANSPARENCY.--

3           A.   A controller shall:

4                   (1)   limit the collection of personal data to  
5   what is adequate, relevant and reasonably necessary in relation  
6   to the purposes for which the personal data is processed, as  
7   disclosed to the consumer;

8                   (2)   except as otherwise provided in the  
9   Consumer Information and Data Protection Act, not process  
10   personal data for purposes that are neither reasonably  
11   necessary to nor compatible with the disclosed purposes for  
12   which the personal data are processed, as disclosed to the  
13   consumer, unless the controller obtains the consumer's consent;

14                  (3)   establish, implement and maintain  
15   reasonable administrative, technical and physical data security  
16   practices to protect the confidentiality, integrity and  
17   accessibility of personal data.  Data security practices shall  
18   be appropriate to the volume and nature of the personal data at  
19   issue;

20                  (4)   not discriminate against a consumer for  
21   exercising any of the consumer rights contained in the Consumer  
22   Information and Data Protection Act, including denying goods or  
23   services, charging different prices or rates for goods or  
24   services or providing a different level of quality of goods and  
25   services to the consumer; provided that nothing in this

.232991.lms

1 subsection shall be construed to require a controller to  
2 provide a product or service that requires the personal data of  
3 a consumer that the controller does not collect or maintain or  
4 to prohibit a controller from offering a different price, rate,  
5 level, quality or selection of goods or services to a consumer,  
6 including offering goods or services for no fee, if the  
7 consumer has exercised the consumer's right to opt out pursuant  
8 to Section 4 of the Consumer Information and Data Protection  
9 Act or the offer is related to a consumer's voluntary  
10 participation in a bona fide loyalty, rewards, premium  
11 features, discounts or club card program; and

12 (5) not process sensitive personal data  
13 concerning a consumer without obtaining the consumer's consent  
14 or, in the case of the processing of sensitive personal data  
15 concerning a child, without processing personal data in  
16 accordance with the federal Children's Online Privacy  
17 Protection Act of 1998.

18 B. Any provision of a contract or agreement that  
19 purports to waive or limit consumer rights pursuant to the  
20 Consumer Information and Data Protection Act shall be deemed  
21 contrary to public policy and shall be void and unenforceable.

22 C. A controller shall provide consumers with a  
23 reasonably accessible, clear and meaningful privacy notice that  
24 includes:

25 (1) the categories of personal data processed

1 by the controller;

2 (2) the purpose for processing personal data;

3 (3) how consumers may exercise their consumer  
4 rights, including how a consumer may appeal a controller's  
5 decision with regard to the consumer's request;

6 (4) the categories of personal data that the  
7 controller shares with third parties, if any;

8 (5) the categories of third parties, if any,  
9 with which the controller shares personal data; and

10 (6) an active email address or other online  
11 mechanism that the consumer may use to contact the controller.

12 D. If a controller sells personal data to third  
13 parties or processes personal data for targeted advertising,  
14 the controller shall clearly and conspicuously disclose that  
15 processing, as well as the manner in which a consumer may  
16 exercise the right to opt out of that processing.

17 E. A controller shall establish, and shall describe  
18 in a privacy notice, one or more secure and reliable means for  
19 consumers to submit a request to exercise their consumer rights  
20 under the Consumer Information and Data Protection Act. The  
21 means shall take into account the ways in which consumers  
22 normally interact with the controller, the need for secure and  
23 reliable communication of the requests and the ability of the  
24 controller to authenticate the identity of the consumer making  
25 the request. Controllers shall not require a consumer to

.232991.lms



1 create a new account in order to exercise consumer rights  
2 pursuant to Section 4 of the Consumer Information and Data  
3 Protection Act but may require a consumer to use an existing  
4 account.

5 F. A controller shall not process any personal data  
6 collected from a child:

7 (1) for the purposes of targeted advertising,  
8 the sale of such personal data or profiling in furtherance of  
9 decisions that produce legal or similarly significant effects  
10 concerning a consumer;

11 (2) unless the processing is reasonably  
12 necessary to provide the online service, product or feature;

13 (3) for any processing purpose other than the  
14 processing purpose that the controller disclosed at the time  
15 the controller collected personal data or that is reasonably  
16 necessary for and compatible with the disclosed purpose; or

17 (4) for longer than is reasonably necessary to  
18 provide the online service, product or feature.

19 G. A controller shall not collect precise  
20 geolocation data from a child unless:

21 (1) the precise geolocation data are  
22 reasonably necessary for the controller to provide an online  
23 service, product or feature, and, if data are necessary to  
24 provide the online service, product or feature, the controller  
25 shall only collect data for the time necessary to provide the

.232991.lms

1 online service, product or feature; and

2 (2) the controller provides to the child a  
3 signal indicating that the controller is collecting precise  
4 geolocation data, which signal shall be available to the child  
5 for the entire duration of data collection.

6 H. A controller shall not engage in the activities  
7 described in Subsections F and G of this section unless the  
8 controller obtains consent from the child's parent or legal  
9 guardian in accordance with the federal Children's Online  
10 Privacy Protection Act of 1998.

11 SECTION 7. [NEW MATERIAL] DATA CONTROLLER  
12 RESPONSIBILITIES--ONLINE SERVICE, PRODUCT OR FEATURE.--

13 A. Each controller that offers an online service,  
14 product or feature to a consumer who is a minor younger than  
15 the age of eighteen, whom the controller has actual knowledge  
16 or willfully disregards that the consumer is younger than the  
17 age of eighteen, shall use reasonable care to avoid any  
18 heightened risk of harm to minors younger than the age of  
19 eighteen caused by the online service, product or feature.

20 B. Subject to the consent requirement established  
21 in Subsection C of this section, a controller that offers an  
22 online service, product or feature to a consumer whom the  
23 controller has actual knowledge or willfully disregards is a  
24 minor younger than the age of eighteen shall not:

25 (1) process personal data of a minor younger

.232991.lms

1 than the age of eighteen for the purposes of:

2 (a) targeted advertising;

3 (b) any sale of personal data; or

4 (c) profiling in furtherance of any

5 fully automated decision made by the controller that produces a  
6 legal or similarly significant effect concerning the provision  
7 or denial by the controller of financial or lending services,  
8 housing, insurance, education enrollment or opportunity,  
9 criminal justice, employment opportunity, health care services  
10 or access to essential goods or services, unless processing is  
11 reasonably necessary to provide the online service, product or  
12 feature, or for any processing purpose other than the  
13 processing purpose that the controller disclosed at the time  
14 the controller collected the personal data, or that is  
15 reasonably necessary for, and compatible with, the processing  
16 purpose described in this subsection, or for longer than is  
17 reasonably necessary to provide the online service, product or  
18 feature; or

19 (2) use any system design feature to  
20 significantly increase, sustain or extend any minor younger  
21 than the age of eighteen's use of such online service, product  
22 or feature. The provisions of this subsection shall not apply  
23 to any service or application that is used by and under the  
24 direction of an educational entity, including a learning  
25 management system or a student engagement program.

.232991.lms

1 C. A controller that offers an online service,  
2 product or feature to a consumer whom the controller has actual  
3 knowledge or willfully disregards is a minor younger than the  
4 age of eighteen shall not engage in the activities described in  
5 Subsections B and D of this section unless the controller  
6 obtains the consent of the minor younger than the age of  
7 eighteen, or, if the minor is a child, the consent of the  
8 child's parent or legal guardian. A controller that complies  
9 with the verifiable parental consent requirements established  
10 in the federal Children's Online Privacy Protection Act of 1998  
11 and the regulations, rules, guidance and exemptions adopted  
12 pursuant to that act shall be deemed to have satisfied any  
13 requirement to obtain parental consent under this section.

14 D. Subject to the consent requirement established  
15 in Subsection C of this section, a controller that offers an  
16 online service, product or feature to a consumer whom the  
17 controller has actual knowledge or willfully disregards is a  
18 minor younger than the age of eighteen shall not collect the  
19 minor's precise geolocation data unless:

20 (1) precise geolocation data are reasonably  
21 necessary for the controller to provide the online service,  
22 product or feature and, if the data are necessary to provide  
23 the online service, product or feature, the controller may only  
24 collect the data for the time necessary to provide the online  
25 service, product or feature; and

.232991.lms

1 (2) the controller provides to the minor a  
2 signal indicating that the controller is collecting the precise  
3 geolocation data, which signal shall be available to the minor  
4 for the entire duration of such collection.

5 E. A controller that offers an online service,  
6 product or feature to a consumer whom the controller has actual  
7 knowledge or willfully disregards is a minor younger than the  
8 age of eighteen shall not:

9 (1) provide a consent mechanism that is  
10 designed to substantially subvert or impair, or is manipulated  
11 with the effect of substantially subverting or impairing, user  
12 autonomy, decision making or choice; or

13 (2) except as provided in Subsection F of this  
14 section, offer any direct messaging apparatus for use by a  
15 minor without providing readily accessible and easy-to-use  
16 safeguards to limit the ability of adults to send unsolicited  
17 communications to a minor with whom they are not connected.

18 F. The provisions of Paragraph (2) of Subsection E  
19 of this section shall not apply to services when the  
20 predominant or exclusive function is:

21 (1) email; or

22 (2) direct messaging consisting of text,  
23 photos or videos that are sent between devices by electronic  
24 means if messages are:

25 (a) shared between the sender and the

1 recipient;

2 (b) only visible to the sender and the  
3 recipient; and

4 (c) not posted publicly.

5 SECTION 8. [NEW MATERIAL] DATA CONTROLLER  
6 RESPONSIBILITIES--ONLINE SERVICE, PRODUCT OR FEATURE--DATA  
7 PROTECTION ASSESSMENTS, REVIEW AND RECORDKEEPING.--

8 A. A controller that, on or after one year after  
9 the effective date of this section, offers an online service,  
10 product or feature to a consumer whom the controller has actual  
11 knowledge or willfully disregards is a minor younger than the  
12 age of eighteen shall conduct a data protection assessment for  
13 the online service, product or feature:

14 (1) in a manner that is consistent with  
15 Section 7 of the Consumer Information and Data Protection Act;  
16 and

17 (2) that addresses:

18 (a) the purpose of the online service,  
19 product or feature;

20 (b) the categories of minors' personal  
21 data that the online service, product or feature processes;

22 (c) the purposes for which the  
23 controller processes minors' personal data with respect to the  
24 online service, product or feature; and

25 (d) any heightened risk of harm to

.232991.lms

1 minors that is a reasonably foreseeable result of offering the  
2 online service, product or feature to minors.

3 B. A controller that conducts a data protection  
4 assessment pursuant to Subsection A of this section shall:

5 (1) review the data protection assessment as  
6 necessary to account for any material change to the processing  
7 operations of the online service, product or feature that is  
8 the subject of the data protection assessment; and

9 (2) maintain documentation concerning the data  
10 protection assessment for the longer of:

11 (a) the three-year period beginning on  
12 the date on which the processing operations cease; or

13 (b) as long as the controller offers the  
14 online service, product or feature.

15 C. If a controller conducts a data protection  
16 assessment for the purpose of complying with another applicable  
17 law or regulation, the data protection assessment shall be  
18 deemed to satisfy the requirements established in this section  
19 if the data protection assessment is reasonably similar in  
20 scope and effect to the data protection assessment that would  
21 otherwise be conducted pursuant to this section.

22 D. If a controller conducts a data protection  
23 assessment pursuant to Subsection A of this section and  
24 determines that the online service, product or feature that is  
25 the subject of the assessment poses a heightened risk of harm

1 to minors, the controller shall establish and implement a plan  
2 to mitigate or eliminate the risk.

3 E. Data protection assessments shall be  
4 confidential and shall be exempt from disclosure under the  
5 Inspection of Public Records Act. To the extent that any  
6 information contained in a data protection assessment disclosed  
7 to the attorney general includes information subject to  
8 attorney-client privilege or work product protection, the  
9 disclosure shall not constitute a waiver of the privilege or  
10 protection.

11 SECTION 9. [NEW MATERIAL] RESPONSIBILITIES OF CONTROLLER  
12 AND PROCESSOR.--

13 A. A processor shall adhere to the instructions of  
14 a controller and shall assist the controller in meeting the  
15 controller's obligations under the Consumer Information and  
16 Data Protection Act. Assistance shall include:

17 (1) taking into account the nature of  
18 processing and the information available to the processor, by  
19 appropriate technical and organizational measures, insofar as  
20 this is reasonably practicable, to fulfill the controller's  
21 obligation to respond to consumer rights requests pursuant to  
22 Section 4 of the Consumer Information and Data Protection Act;

23 (2) taking into account the nature of  
24 processing and the information available to the processor, by  
25 assisting the controller in meeting the controller's

.232991.lms



1 obligations regarding the security of processing the personal  
2 data and the notification of a breach of security of the system  
3 of the processor pursuant to the Consumer Information and Data  
4 Protection Act to meet the controller's obligations; and

5 (3) providing necessary information to enable  
6 the controller to conduct and document data protection  
7 assessments pursuant to the Consumer Information and Data  
8 Protection Act.

9 B. A contract between a controller and a processor  
10 shall govern the processor's data processing procedures with  
11 respect to processing performed on behalf of the controller.  
12 The contract shall be binding and clearly set forth  
13 instructions for processing data, the nature and purpose of  
14 processing, the type of data subject to processing, the  
15 duration of processing and the rights and obligations of both  
16 parties. The contract shall also include requirements that the  
17 processor shall:

18 (1) ensure that each person processing  
19 personal data is subject to a duty of confidentiality with  
20 respect to the personal data;

21 (2) at the controller's direction, delete or  
22 return all personal data to the controller as requested at the  
23 end of the provision of services, unless retention of the  
24 personal data is required by law;

25 (3) upon the reasonable request of the

1 controller, make available to the controller all information in  
2 the processor's possession necessary to demonstrate the  
3 processor's compliance with the obligations in the Consumer  
4 Information and Data Protection Act;

5 (4) allow, and cooperate with, reasonable  
6 assessments by the controller or the controller's designated  
7 assessor; alternatively, the processor may arrange for a  
8 qualified and independent assessor to conduct an assessment of  
9 the processor's policies and technical and organizational  
10 measures in support of the obligations under the Consumer  
11 Information and Data Protection Act using an appropriate and  
12 accepted control standard or framework and assessment procedure  
13 for those assessments. The processor shall provide a report of  
14 the assessment to the controller upon request; and

15 (5) engage any subcontractor pursuant to a  
16 written contract in accordance with this section that requires  
17 the subcontractor to meet the obligations of the processor with  
18 respect to the personal data.

19 C. Nothing in this section shall be construed to  
20 relieve a controller or a processor from the liabilities  
21 imposed on it by the controller's or processor's role in the  
22 processing relationship as provided in the Consumer Information  
23 and Data Protection Act.

24 D. Determining whether a person is acting as a  
25 controller or processor with respect to a specific processing

1 of personal data is a fact-based determination that depends  
2 upon the context in which personal data are to be processed. A  
3 processor that continues to adhere to a controller's  
4 instructions with respect to a specific processing of personal  
5 data remains a processor.

6 SECTION 10. [NEW MATERIAL] DATA PROTECTION ASSESSMENTS.--

7 A. A controller shall conduct and document a data  
8 protection assessment of each of the following processing  
9 activities involving personal data:

10 (1) the processing of personal data for  
11 purposes of targeted advertising;

12 (2) the sale of personal data;

13 (3) the processing of personal data for  
14 purposes of profiling, where such profiling presents a  
15 reasonably foreseeable risk of:

16 (a) unfair or deceptive treatment of or  
17 unlawful disparate impact on consumers;

18 (b) financial, physical or reputational  
19 injury to consumers;

20 (c) a physical or other intrusion upon  
21 the solitude or seclusion, or the private affairs or concerns,  
22 of consumers where such intrusion would be offensive to a  
23 reasonable person; or

24 (d) other substantial injury to  
25 consumers;

1 (4) the processing of sensitive data; and  
2 (5) any processing activities involving  
3 personal data that present a heightened risk of harm to  
4 consumers.

5 B. Data protection assessments conducted pursuant  
6 to Subsection A of this section shall identify and weigh the  
7 benefits that may flow, directly and indirectly, from the  
8 processing to the controller, the consumer, other stakeholders  
9 and the public against the potential risks to the rights of the  
10 consumer associated with the processing, as mitigated by  
11 safeguards that can be employed by the controller to reduce  
12 risks. The use of de-identified data and the reasonable  
13 expectations of consumers, as well as the context of the  
14 processing and the relationship between the controller and the  
15 consumer whose personal data will be processed, shall be  
16 factored into this assessment by the controller.

17 C. The attorney general may request, pursuant to a  
18 civil investigative demand, that a controller disclose a data  
19 protection assessment that is relevant to an investigation  
20 conducted by the attorney general, and the controller shall  
21 make the data protection assessment available to the attorney  
22 general. The attorney general may evaluate the data protection  
23 assessment for compliance with the responsibilities set forth  
24 in Subsection A of this section.

25 D. A single data protection assessment may address

1 a comparable set of processing operations that include similar  
2 activities.

3 E. Data protection assessment requirements shall  
4 apply to processing activities created or generated after the  
5 effective date of this section and are not retroactive.

6 SECTION 11. [NEW MATERIAL] PROCESSING DE-IDENTIFIED  
7 DATA.--

8 A. The controller in possession of de-identified  
9 data shall:

10 (1) take reasonable measures to ensure that  
11 the data cannot be associated with an identified or  
12 identifiable individual;

13 (2) publicly commit to maintaining and using  
14 de-identified data without attempting to re-identify the data;  
15 and

16 (3) contractually obligate any recipients of  
17 the de-identified data to comply with all provisions of the  
18 Consumer Information and Data Protection Act.

19 B. Nothing in the Consumer Information and Data  
20 Protection Act shall be construed to require a controller or  
21 processor to re-identify de-identified data or pseudonymous  
22 data or maintain data in identifiable form, or collect, obtain,  
23 retain or access any data or technology, in order to be capable  
24 of associating an authentic consumer request with personal  
25 data.

.232991.lms

1 C. Nothing in the Consumer Information and Data  
2 Protection Act shall be construed to require a controller or  
3 processor to comply with an authentic consumer rights request,  
4 pursuant to Section 4 of the Consumer Information and Data  
5 Protection Act, if:

6 (1) the controller is not reasonably capable  
7 of associating the request with the personal data or it would  
8 be unreasonably burdensome for the controller to associate the  
9 request with the personal data;

10 (2) the controller does not use the personal  
11 data to recognize or respond to the specific consumer who is  
12 the subject of the personal data or associate the personal data  
13 with other personal data about the same specific consumer; and

14 (3) the controller does not sell the personal  
15 data to a third party or otherwise voluntarily disclose the  
16 personal data to a third party other than a processor, except  
17 as otherwise permitted in this section.

18 D. The consumer rights contained in Section 4 of  
19 the Consumer Information and Data Protection Act shall not  
20 apply to pseudonymous data in cases where the controller is  
21 able to demonstrate that any information necessary to identify  
22 the consumer is kept separately and is subject to effective  
23 technical and organizational controls that prevent the  
24 controller from accessing the information.

25 E. A controller that discloses pseudonymous data or

1 de-identified data shall exercise reasonable oversight to  
2 monitor compliance with any contractual commitments to which  
3 the pseudonymous data or de-identified data are subject and  
4 shall take appropriate steps to address any breaches of those  
5 contractual commitments.

6 SECTION 12. [NEW MATERIAL] LIMITATIONS.--

7 A. Nothing in the Consumer Information and Data  
8 Protection Act shall be construed to restrict a controller's or  
9 processor's ability to:

10 (1) comply with a civil, criminal or  
11 regulatory inquiry, investigation, subpoena or summons by  
12 federal, state, local or other governmental authorities;

13 (2) cooperate with law enforcement agencies  
14 concerning conduct or activity that the controller or processor  
15 reasonably and in good faith believes may violate federal,  
16 state or local laws, rules or regulations;

17 (3) investigate, establish, exercise, prepare  
18 for or defend legal claims;

19 (4) provide a product or service specifically  
20 requested by a consumer, perform a contract to which the  
21 consumer is a party, including fulfilling the terms of a  
22 written warranty, or take steps at the request of the consumer  
23 prior to entering into a contract;

24 (5) take immediate steps to protect an  
25 interest that is essential for the life or physical safety of

.232991.lms

1 the consumer or of another natural person and where the  
2 processing cannot be manifestly based on another legal basis;

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

7 (7) preserve the integrity or security of  
8 systems;

9 (8) report those responsible for actions  
10 contrary to the Consumer Information and Data Protection Act;

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

16 (a) if the deletion of the information  
17 is likely to provide substantial benefits that do not  
18 exclusively accrue to the controller;

19 (b) that the expected benefits of the  
20 research outweigh the privacy risks; and

21 (c) if the controller has implemented  
22 reasonable safeguards to mitigate privacy risks associated with  
23 research, including any risks associated with re-  
24 identification; or

25 (10) assist another controller, processor or



1 third party with any of the obligations under this subsection.

2 B. The obligations imposed on controllers or  
3 processors under the Consumer Information and Data Protection  
4 Act shall not restrict a controller's or processor's ability to  
5 collect, use or retain data to:

6 (1) conduct internal research to develop,  
7 improve or repair products, services or technology;

8 (2) effectuate a product recall;

9 (3) identify and repair technical errors that  
10 impair existing or intended functionality; or

11 (4) perform internal operations that are  
12 reasonably aligned with the expectations of the consumer or  
13 reasonably anticipated based on the consumer's existing  
14 relationship with the controller or are otherwise compatible  
15 with processing data in furtherance of the provision of a  
16 product or service specifically requested by a consumer or the  
17 performance of a contract to which the consumer is a party.

18 C. A controller or processor that discloses  
19 personal data to a third-party controller or processor, in  
20 compliance with the requirements of the Consumer Information  
21 and Data Protection Act, is not in violation of that act if the  
22 third-party controller or processor that receives and processes  
23 the personal data is in violation of that act; provided that,  
24 at the time of disclosing the personal data, the disclosing  
25 controller or processor did not have actual knowledge that the

.232991.lms

1 recipient intended to commit a violation. A third-party  
2 controller or processor receiving personal data from a  
3 controller or processor in compliance with the requirements of  
4 that act is not in violation for the transgressions of the  
5 controller or processor from which it receives personal data.

6 D. Personal data processed by a controller pursuant  
7 to this section shall not be processed for any purpose other  
8 than those expressly listed in this section unless otherwise  
9 allowed by the Consumer Information and Data Protection Act.

10 Personal data processed by a controller pursuant to this  
11 section may be processed to the extent that such processing is:

12 (1) reasonably necessary and proportionate to  
13 the purposes listed in this section; and

14 (2) adequate, relevant and limited to what is  
15 necessary in relation to the specific purposes listed in this  
16 section. Personal data collected, used or retained pursuant to  
17 Subsection B of this section shall, where applicable, take into  
18 account the nature and purpose or purposes of data collection,  
19 use or retention. Data shall be subject to reasonable  
20 administrative, technical and physical measures to protect the  
21 confidentiality, integrity and accessibility of the personal  
22 data and to reduce reasonably foreseeable risks of harm to  
23 consumers relating to the collection, use or retention of  
24 personal data.

25 E. If a controller processes personal data pursuant

.232991.lms

1 to an exemption in this section, the controller bears the  
2 burden of demonstrating that processing qualifies for the  
3 exemption and complies with the requirements in Subsection D of  
4 this section.

5 F. Processing personal data for the purposes  
6 expressly identified in Subsection A of this section shall not  
7 solely make an entity a controller with respect to that  
8 processing.

9 SECTION 13. [NEW MATERIAL] DATA IN THE POSSESSION OF  
10 FEDERAL AGENCIES.--

11 A. A person shall not share, disclose, re-disclose  
12 or otherwise disseminate a covered resident's sensitive data in  
13 the possession of a federal agency without the consent of the  
14 covered resident, except where that disclosure is pursuant to a  
15 law enacted by congress.

16 B. A third party that receives sensitive data of a  
17 covered resident from the federal government or its agents,  
18 without express authorization by a law enacted by congress  
19 permitting disclosure, upon request by the covered resident or  
20 the attorney general, shall:

21 (1) delete the sensitive data in its  
22 possession; and

23 (2) disclose the source from which the  
24 sensitive data were obtained.

25 C. A person who receives a request or demand for a

.232991.lms

1 covered resident's sensitive data in the possession of a  
2 federal agency without the consent of the covered resident  
3 shall not share, disclose, re-disclose or otherwise disseminate  
4 sensitive data without first receiving an order of a court of  
5 competent jurisdiction that the disclosure is pursuant to a law  
6 enacted by congress.

7 D. The attorney general may enforce the provisions  
8 of this section and may issue a civil investigation demand  
9 whenever the attorney general has reasonable cause to believe  
10 that a person has engaged in, is engaging in or is about to  
11 engage in a violation of this section. A person issued an  
12 investigative demand shall produce the material sought and  
13 shall permit it to be copied and inspected by the attorney  
14 general. The demand of the attorney general and any material  
15 produced in response to it shall not be a matter of public  
16 record and shall not be published by the attorney general  
17 except by order of the court.

18 E. Upon reasonable belief that there has been a  
19 violation of this section, the attorney general:

20 (1) may bring an action in the name of the  
21 state to enforce the provisions of this section;

22 (2) may petition the court for injunctive  
23 relief; and

24 (3) shall not be required to post bond when  
25 seeking a temporary or permanent injunction.

.232991.lms

1           SECTION 14.   [NEW MATERIAL] ENFORCEMENT--CIVIL

2   PENALTIES.--

3           A.   The attorney general may enforce the provisions  
4   of the Consumer Information and Data Protection Act.

5           B.   Prior to initiating an action under the Consumer  
6   Information and Data Protection Act other than as specified in  
7   Section 13 of that act, the attorney general shall provide a  
8   controller or processor thirty days' written notice identifying  
9   the specific provisions of the Consumer Information and Data  
10   Protection Act that the attorney general alleges have been or  
11   are being violated.  If within the thirty-day period the  
12   controller or processor cures the noticed violation and  
13   provides the attorney general an express written statement that  
14   the alleged violations have been cured and that no further  
15   violations shall occur, no action shall be initiated against  
16   the controller or processor.

17           C.   If a controller or processor continues to  
18   violate the Consumer Information and Data Protection Act  
19   following the cure period in Subsection B of this section or  
20   breaches an express written statement provided to the attorney  
21   general under that subsection, the attorney general may  
22   initiate an action and may seek an injunction to restrain any  
23   violations of that act and civil penalties of up to ten  
24   thousand dollars (\$10,000) for each violation under that act.

25           D.   The attorney general may recover reasonable

.232991.lms

1 attorney fees and costs of investigation and enforcement  
2 whenever a court finds a violation of the Consumer Information  
3 and Data Protection Act.

4 E. Nothing in the Consumer Information and Data  
5 Protection Act shall be construed as providing the basis for,  
6 or being subject to, a private right of action for violations  
7 of that act or under any other law.

8 SECTION 15. [NEW MATERIAL] SEVERABILITY.--

9 A. Every provision, section, subsection, sentence,  
10 clause, phrase or word in the Consumer Information and Data  
11 Protection Act, and every application of the provisions in that  
12 act, are severable from each other.

13 B. If an application of a provision in the Consumer  
14 Information and Data Protection Act to a person, group of  
15 persons or circumstances is found by a court to be invalid or  
16 unconstitutional, the remaining applications of that provision  
17 to all other persons and circumstances shall be severed and  
18 shall not be affected. All constitutionally valid applications  
19 of the Consumer Information and Data Protection Act shall be  
20 severed from any applications that a court finds to be invalid,  
21 leaving the valid applications in force, because it is the  
22 legislature's intent and priority that the valid applications  
23 be allowed to stand alone. Even if a reviewing court finds a  
24 provision of the Consumer Information and Data Protection Act  
25 to impose an undue burden in a large or substantial fraction of

1 relevant cases, the applications that do not present an undue  
2 burden shall be severed from the remaining applications, shall  
3 remain in force and shall be treated as if the legislature had  
4 enacted a statute limited to the persons, group of persons or  
5 circumstances for which the statute's application does not  
6 present an undue burden.

7 C. If any court declares or finds a provision of  
8 the Consumer Information and Data Protection Act facially  
9 unconstitutional, when discrete applications of that provision  
10 can be enforced against a person, group of persons or  
11 circumstances without violating the United States constitution  
12 and the constitution of New Mexico, those applications shall be  
13 severed from all remaining applications of the provision, and  
14 the provision shall be interpreted as if the legislature had  
15 enacted a provision limited to the persons, group of persons or  
16 circumstances for which the provision's application will not  
17 violate the United States constitution and the constitution of  
18 New Mexico.

19 D. The legislature further declares that it would  
20 have enacted the Consumer Information and Data Protection Act,  
21 and each provision, section, subsection, sentence, clause,  
22 phrase or word, and all constitutional applications of that  
23 act, regardless of the fact that any provision, section,  
24 subsection, sentence, clause, phrase or word or application of  
25 that act were to be declared unconstitutional or to represent

1 an undue burden.

2 E. If any provision of the Consumer Information and  
3 Data Protection Act is found by any court to be  
4 unconstitutionally vague, then the applications of that  
5 provision that do not present constitutional vagueness problems  
6 shall be severed and remain in force.

7 SECTION 16. EFFECTIVE DATES.--

8 A. The effective date of the provisions of Sections  
9 1, 2 and 13 through 15 of this act is July 1, 2026.

10 B. The effective date of the provisions of Sections  
11 3 through 12 of this act is July 1, 2027.

12 - 48 -  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25