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 and Rebecca Dow

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

(1) a digital or physical photograph;

(2) an audio or a video recording; or

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

D. "business associate" has the same meaning as

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

nonprofit organization or government agency;

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

(3) delivery or use of a physical product;

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

Z. "profiling" means a form of automated processing

underscored material = new
[~~bracketed material~~] = delete

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

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

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

CC. "publicly available information" means information that:

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

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

DD. "reproductive or sexual health care" means

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

GG. "sensitive data" means personal data that

underscored material = new
[~~bracketed material~~] = delete

include:

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

(2) consumer health data;

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

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

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

(6) personal data collected from a child;

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

(8) precise geolocation data; and

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

B. A person shall not:

(1) provide an employee or a contractor with

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

(4) nonprofit organization;

(5) institution of higher education;

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

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

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

(9) information and documents created for

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

(18) personal data processed or maintained:

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

(5) opt out of the processing of the personal

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

(5) a controller that has obtained personal

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

C of this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to Subsection A of this section. Within sixty days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

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

underscored material = new
[~~bracketed material~~] = delete

SECTION 6. [NEW MATERIAL] DATA CONTROLLER RESPONSIBILITIES--TRANSPARENCY.--

A. A controller shall:

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

(1) the categories of personal data processed

underscored material = new
[~~bracketed material~~] = delete

by the controller;

(2) the purpose for processing personal data;

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

online service, product or feature; and

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

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

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

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

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

(1) process personal data of a minor younger

underscored material = new
[~~bracketed material~~] = delete

than the age of eighteen for the purposes of:

(a) targeted advertising;

(b) any sale of personal data; or

(c) profiling in furtherance of any fully automated decision made by the controller that produces a legal or similarly significant effect concerning the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services, unless processing is reasonably necessary to provide the online service, product or feature, or for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the personal data, or that is reasonably necessary for, and compatible with, the processing purpose described in this subsection, or for longer than is reasonably necessary to provide the online service, product or feature; or

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

(1) email; or

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

(a) shared between the sender and the

underscored material = new
[~~bracketed material~~] = delete

recipient;

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

(c) not posted publicly.

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

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

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

(2) that addresses:

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

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

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

(d) any heightened risk of harm to

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

(3) upon the reasonable request of the

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

(2) the sale of personal data;

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

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

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

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

(d) other substantial injury to consumers;

underscored material = new
[~~bracketed material~~] = delete

(4) the processing of sensitive data; and

(5) any processing activities involving personal data that present a heightened risk of harm to consumers.

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

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

D. A single data protection assessment may address

underscored material = new
[~~bracketed material~~] = delete

a comparable set of processing operations that include similar activities.

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

E. A controller that discloses pseudonymous data or

underscored material = new
[~~bracketed material~~] = delete

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

SECTION 12. [NEW MATERIAL] LIMITATIONS.--

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

(7) preserve the integrity or security of systems;

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

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

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

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

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

(10) assist another controller, processor or

third party with any of the obligations under this subsection.

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

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

(2) effectuate a product recall;

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

D. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by the Consumer Information and Data Protection Act. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

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

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

E. If a controller processes personal data pursuant

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

D. The attorney general may recover reasonable

underscored material = new
[~~bracketed material~~] = delete

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

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

SECTION 15. [NEW MATERIAL] SEVERABILITY.--

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

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

underscored material = new
[~~bracketed material~~] = delete

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

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

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

underscored material = new
[~~bracketed material~~] = delete

an undue burden.

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

SECTION 16. EFFECTIVE DATES.--

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

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

underscored material = new
[~~bracketed material~~] = delete