LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: C.R. Gilbert ₵
₵ 02-25-22 12:44 PM ₵

Senator Kirk A. Cullimore proposes the following substitute bill:

CONSUMER PRIVACY ACT

2022 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kirk A. Cullimore

House Sponsor: Brady Brammer

LONG TITLE

General Description:

This bill enacts the Utah Consumer Privacy Act.

Highlighted Provisions:

This bill:

- ▸ defines terms;
- ▸ provides consumers the right to:
  - • access and delete certain personal data maintained by certain businesses; and
  - • opt out of the collection and use of personal data for certain purposes;
- ▸ requires certain businesses that control and process consumers' personal data to:
  - • safeguard consumers' personal data;
  - • provide clear information to consumers regarding how the consumers' personal data are used; and
  - • accept and comply with a consumer's request to exercise the consumer's rights under this bill;
- ▸ creates a right for a consumer to know what personal data a business collects, how the business uses the personal data, and whether the business sells the personal data;
- ▸ upon request and subject to exceptions, requires a business to delete a consumer's personal data or stop selling the consumer's personal data;

- allows the Division of Consumer Protection to accept and investigate consumer complaints regarding the processing of personal data;
- authorizes the Office of the Attorney General to take enforcement action and impose penalties; and
- makes technical changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

This bill provides a special effective date.

Utah Code Sections Affected:

AMENDS:

13-2-1, as last amended by Laws of Utah 2021, Chapter 266

ENACTS:

13-61-101, Utah Code Annotated 1953
13-61-102, Utah Code Annotated 1953
13-61-103, Utah Code Annotated 1953
13-61-201, Utah Code Annotated 1953
13-61-202, Utah Code Annotated 1953
13-61-203, Utah Code Annotated 1953
13-61-301, Utah Code Annotated 1953
13-61-302, Utah Code Annotated 1953
13-61-303, Utah Code Annotated 1953
13-61-304, Utah Code Annotated 1953
13-61-305, Utah Code Annotated 1953
13-61-401, Utah Code Annotated 1953
13-61-402, Utah Code Annotated 1953
13-61-403, Utah Code Annotated 1953
13-61-404, Utah Code Annotated 1953

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **13-2-1** is amended to read:

13-2-1. Consumer protection division established -- Functions.

(1) There is established within the Department of Commerce the Division of Consumer Protection.

(2) The division shall administer and enforce the following:

(a) Chapter 5, Unfair Practices Act;

(b) Chapter 10a, Music Licensing Practices Act;

(c) Chapter 11, Utah Consumer Sales Practices Act;

(d) Chapter 15, Business Opportunity Disclosure Act;

(e) Chapter 20, New Motor Vehicle Warranties Act;

(f) Chapter 21, Credit Services Organizations Act;

(g) Chapter 22, Charitable Solicitations Act;

(h) Chapter 23, Health Spa Services Protection Act;

(i) Chapter 25a, Telephone and Facsimile Solicitation Act;

(j) Chapter 26, Telephone Fraud Prevention Act;

(k) Chapter 28, Prize Notices Regulation Act;

(l) Chapter 32a, Pawnshop and Secondhand Merchandise Transaction Information Act;

(m) Chapter 34, Utah Postsecondary Proprietary School Act;

(n) Chapter 34a, Utah Postsecondary School State Authorization Act;

(o) Chapter 41, Price Controls During Emergencies Act;

(p) Chapter 42, Uniform Debt-Management Services Act;

(q) Chapter 49, Immigration Consultants Registration Act;

(r) Chapter 51, Transportation Network Company Registration Act;

(s) Chapter 52, Residential Solar Energy Disclosure Act;

(t) Chapter 53, Residential, Vocational and Life Skills Program Act;

(u) Chapter 54, Ticket Website Sales Act;

(v) Chapter 56, Ticket Transferability Act; [~~and~~]

(w) Chapter 57, Maintenance Funding Practices Act[~~.~~]; and

(x) Chapter 61, Utah Consumer Privacy Act.

Section 2. Section **13-61-101** is enacted to read:

CHAPTER 61. UTAH CONSUMER PRIVACY ACT

Part 1. General Provisions

13-61-101. Definitions.

As used in this chapter:

(1) "Account" means the Consumer Privacy Restricted Account established in Section 13-61-403.

(2) "Affiliate" means an entity that:

(a) controls, is controlled by, or is under common control with another entity; or

(b) shares common branding with another entity.

(3) "Aggregated data" means information that relates to a group or category of consumers:

(a) from which individual consumer identities have been removed; and

(b) that is not linked or reasonably linkable to any consumer.

(4) "Air carrier" means the same as that term is defined in 49 U.S.C. Sec. 40102.

(5) "Authenticate" means to use reasonable means to determine that a consumer's request to exercise the rights described in Section 13-61-201 is made by the consumer who is entitled to exercise those rights.

(6) (a) "Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics.

(b) "Biometric data" includes data described in Subsection (6)(a) that are:

(i) generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual; or

(ii) captured from a patient in a health care setting.

(c) "Biometric data" does not include:

(i) a physical or digital photograph;

(ii) a video or audio recording;

(iii) data generated from an item described in Subsection (6)(c)(i) or (ii); or

(iv) information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

(7) "Business associate" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(8) "Child" means an individual younger than 13 years old.

(9) "Consent" means an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer.

(10) (a) "Consumer" means an individual who is a resident of the state acting in an individual or household context.

(b) "Consumer" does not include an individual acting in an employment or commercial context.

(11) "Control" or "controlled" as used in Subsection (2) means:

(a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting securities of an entity;

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

(c) the power to exercise controlling influence of the management of an entity.

(12) "Controller" means a person doing business in the state who determines the purposes for which and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others.

(13) "Covered entity" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(14) "Deidentified data" means data that:

(a) cannot reasonably be linked to an identified individual or an identifiable individual; and

(b) are possessed by a controller who:

(i) takes reasonable measures to ensure that a person cannot associate the data with an individual;

(ii) publicly commits to maintain and use the data only in deidentified form and not attempt to reidentify the data; and

(iii) contractually obligates any recipients of the data to comply with the requirements described in Subsections (14)(b)(i) and (ii).

(15) "Director" means the director of the Division of Consumer Protection.

(16) "Division" means the Division of Consumer Protection created in Section 13-2-1.

(17) "Governmental entity" means the same as that term is defined in Section

63G-2-103.

(18) "Health care facility" means the same as that term is defined in Section 26-21-2.

(19) "Health care provider" means the same as that term is defined in Section 26-21-2.

(20) "Identifiable individual" means an individual who can be readily identified, directly or indirectly.

(21) "Institution of higher education" means a public or private institution of higher education.

(22) "Local political subdivision" means the same as that term is defined in Section 11-14-102.

(23) "Nonprofit corporation" means:

(a) the same as that term is defined in Section 16-6a-102; or

(b) a foreign nonprofit corporation as defined in Section 16-6a-102.

(24) (a) "Personal data" means information that is linked or reasonably linkable to an identified individual or an identifiable individual.

(b) "Personal data" does not include deidentified data, aggregated data, or publicly available information.

(25) "Process" means an operation or set of operations performed on personal data, including collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) "Processor" means a person who processes personal data on behalf of a controller.

(27) "Protected health information" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(28) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is:

(a) kept separate from the consumer's personal data; and

(b) subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual.

(29) "Publicly available information" means information that a person:

(a) lawfully obtains from a record of a governmental entity;

(b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or

(c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

(30) "Right" means a consumer right described in Section 13-61-201.

(31) (a) "Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party.

(b) "Sale," "sell," or "sold" does not include:

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

(ii) a controller's disclosure of personal data to an affiliate of the controller;

(iii) considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations;

(iv) the disclosure or transfer of personal data when a consumer directs a controller to:

(A) disclose the personal data; or

(B) interact with one or more third parties;

(v) a consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a child;

(vi) the disclosure of information that the consumer:

(A) intentionally makes available to the general public via a channel of mass media; and

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

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

(32) (a) "Sensitive data" means:

(i) personal data that reveals:

(A) an individual's racial or ethnic origin;

(B) an individual's religious beliefs;

(C) an individual's sexual orientation;

(D) an individual's citizenship or immigration status; or

(E) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;

(ii) the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or

(iii) specific geolocation data.

(b) "Sensitive data" does not include personal data that reveals an individual's:

(i) racial or ethnic origin, if the personal data is processed by a video communication service; or

(ii) if the personal data is processed by a person licensed to provide health care under Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58, Occupations and Professions, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.

(33) (a) "Specific geolocation data" means information derived from technology, including global position system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of 1,750 feet or less.

(b) "Specific geolocation data" does not include:

(i) the content of a communication; or

(ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(34) (a) "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include advertising:

(i) based on a consumer's activities within a controller's website or online application or any affiliated website or online application;

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

(iii) directed to a consumer in response to the consumer's request for information, product, a service, or feedback; or

(iv) processing personal data solely to measure or report advertising:

(A) performance;

(B) reach; or

(C) frequency.

(35) "Third party" means a person other than:

(a) the consumer, controller, or processor; or

(b) an affiliate or contractor of the controller or the processor.

(36) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

Section 3. Section **13-61-102** is enacted to read:

13-61-102. Applicability.

(1) This chapter applies to any controller or processor who:

(a) (i) conducts business in the state; or

(ii) produces a product or service that is targeted to consumers who are residents of the state;

(b) has annual revenue of $25,000,000 or more; and

(c) satisfies one or more of the following thresholds:

(i) during a calendar year, controls or processes personal data of 100,000 or more consumers; or

(ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

(2) This chapter does not apply to:

(a) a governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity;

(b) a tribe;

(c) an institution of higher education;

(d) a nonprofit corporation;

(e) a covered entity;

(f) a business associate;

(g) information that meets the definition of:

(i) protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., and related regulations;

(ii) patient identifying information for purposes of 42 C.F.R. Part 2;

(iii) identifiable private information for purposes of the Federal Policy for the Protection of Human Subjects, 45 C.F.R. Part 46;

(iv) identifiable private information or personal data collected as part of human subjects research pursuant to or under the same standards as:

(A) the good clinical practice guidelines issued by the International Council for Harmonisation; or

(B) the Protection of Human Subjects under 21 C.F.R. Part 50 and Institutional Review Boards under 21 C.F.R. Part 56;

(v) personal data used or shared in research conducted in accordance with one or more of the requirements described in Subsection (2)(g)(iv);

(vi) information and documents created specifically for, and collected and maintained by, a committee listed in Section 26-1-7;

(vii) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. Sec. 11101 et seq., and related regulations;

(viii) patient safety work product for purposes of 42 C.F.R. Part 3; or

(ix) information that is:

(A) deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164; and

(B) derived from any of the health care-related information listed in this Subsection (2)(g);

(h) information originating from, and intermingled to be indistinguishable with, information under Subsection (2)(g) that is maintained by:

(i) a health care facility or health care provider; or

(ii) a program or a qualified service organization as defined in 42 C.F.R. Sec. 2.11;

(i) information used only for public health activities and purposes as described in 45

C.F.R. Sec. 164.512;

(j) (i) an activity by:

(A) a consumer reporting agency, as defined in 15 U.S.C. Sec. 1681a;

(B) a furnisher of information, as set forth in 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in 15 U.S.C. Sec. 1681a; or

(C) a user of a consumer report, as set forth in 15 U.S.C. Sec. 1681b;

(ii) subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. Sec. 1681 et seq.; and

(iii) involving the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's:

(A) credit worthiness;

(B) credit standing;

(C) credit capacity;

(D) character;

(E) general reputation;

(F) personal characteristics; or

(G) mode of living;

(k) a financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., and related regulations;

(l) personal data collected, processed, sold, or disclosed in accordance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Sec. 2721 et seq.;

(m) personal data regulated by the federal Family Education Rights and Privacy Act, 20 U.S.C. Sec. 1232g, and related regulations;

(n) personal data collected, processed, sold, or disclosed in accordance with the federal Farm Credit Act of 1971, 12 U.S.C. Sec. 2001 et seq.;

(o) data that are processed or maintained:

(i) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent the collection and use of the data are related to the individual's role;

(ii) as the emergency contact information of an individual described in Subsection

(2)(o)(i) and used for emergency contact purposes; or

(iii) to administer benefits for another individual relating to an individual described in Subsection (2)(o)(i) and used for the purpose of administering the benefits;

(p) an individual's processing of personal data for purely personal or household purposes; or

(q) an air carrier.

(3) A controller is in compliance with any obligation to obtain parental consent under this chapter if the controller complies with the verifiable parental consent mechanisms under the Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) This chapter does not require a person to take any action in conflict with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., or related regulations.

Section 4. Section **13-61-103** is enacted to read:

13-61-103. Preemption -- Reference to other laws.

(1) This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a local political subdivision regarding the processing of personal data by a controller or processor.

(2) Any reference to federal law in this chapter includes any rules or regulations promulgated under the federal law.

Section 5. Section **13-61-201** is enacted to read:

Part 2. Rights Relating to Personal Data

13-61-201. Consumer rights -- Access -- Deletion -- Portability -- Opt out of certain processing.

(1) A consumer has the right to:

(a) confirm whether a controller is processing the consumer's personal data; and

(b) access the consumer's personal data.

(2) A consumer has the right to delete the consumer's personal data that the consumer provided to the controller.

(3) A consumer has the right to obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that:

(a) to the extent technically feasible, is portable;

(b) to the extent practicable, is readily usable; and

(c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

(4) A consumer has the right to opt out of the processing of the consumer's personal data for purposes of:

(a) targeted advertising; or

(b) the sale of personal data.

(5) Nothing in this section requires a person to cause a breach of security system as defined in Section 13-44-102.

Section 6. Section **13-61-202** is enacted to read:

13-61-202. Exercising consumer rights.

(1) A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.

(2) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.

(3) In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under Title 75, Chapter 5, Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

Section 7. Section **13-61-203** is enacted to read:

13-61-203. Controller's response to requests.

(1) Subject to the other provisions of this chapter, a controller shall comply with a consumer's request under Section 13-61-202 to exercise a right.

(2) (a) Within 45 days after the day on which a controller receives a request to exercise a right, the controller shall:

(i) take action on the consumer's request; and

(ii) inform the consumer of any action taken on the consumer's request.

(b) The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller.

(c) If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall:

(i) inform the consumer of the extension, including the length of the extension; and

(ii) provide the reasons the extension is reasonably necessary as described in Subsection (2)(b).

(d) The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.

(3) If, in accordance with this section, a controller chooses not to take action on a consumer's request, the controller shall within 45 days after the day on which the controller receives the request, inform the consumer of the reasons for not taking action.

(4) (a) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same 12-month period.

(b) (i) Notwithstanding Subsection (4)(a), a controller may charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request, if:

(A) the request is excessive, repetitive, technically infeasible, or manifestly unfounded;

(B) the controller reasonably believes the primary purpose in submitting the request was something other than exercising a right; or

(C) the request, individually or as part of an organized effort, harasses, disrupts, or imposes undue burden on the resources of the controller's business.

(ii) A controller that charges a fee or refuses to act in accordance with this Subsection (4)(b) bears the burden of demonstrating the request satisfied one or more of the criteria described in Subsection (4)(b)(i).

(5) If a controller is unable to authenticate a consumer request to exercise a right described in Section 13-61-201 using commercially reasonable efforts, the controller:

(a) is not required to comply with the request; and

(b) may request that the consumer provide additional information reasonably necessary to authenticate the request.

Section 8. Section **13-61-301** is enacted to read:

Part 3. Requirements for Controllers and Processors

13-61-301. Responsibility according to role.

(1) A processor shall:

(a) adhere to the controller's instructions; and

(b) taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system described in Section 13-44-202.

(2) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that:

(a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations;

(b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and

(c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

(3) (a) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed.

(b) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

Section 9. Section **13-61-302** is enacted to read:

13-61-302. Responsibilities of controllers -- Transparency -- Purpose specification and data minimization -- Consent for secondary use -- Security -- Nondiscrimination -- Nonretaliation -- Nonwaiver of consumer rights.

(1) (a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(i) the categories of personal data processed by the controller;

(ii) the purposes for which the categories of personal data are processed;

(iii) how consumers may exercise a right;

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

(v) the categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

(i) sale of the consumer's personal data; or

(ii) processing for targeted advertising.

(2) (a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:

(i) protect the confidentiality and integrity of personal data; and

(ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.

(b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

(3) Except as otherwise provided in this chapter, a controller may not process sensitive data collected from a consumer without:

(a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or

(b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) (a) A controller may not discriminate against a consumer for exercising a right by:

(i) denying a good or service to the consumer;

(ii) charging the consumer a different price or rate for a good or service; or

(iii) providing the consumer a different level of quality of a good or service.

(b) This Subsection (4) does not prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if:

(i) the consumer has opted out of targeted advertising; or

(ii) the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(5) A controller is not required to provide a product, service, or functionality to a consumer if:

(a) the consumer's personal data are or the processing of the consumer's personal data is reasonably necessary for the controller to provide the consumer the product, service, or functionality; and

(b) the consumer does not:

(i) provide the consumer's personal data to the controller; or

(ii) allow the controller to process the consumer's personal data.

(6) Any provision of a contract that purports to waive or limit a consumer's right under this chapter is void.

Section 10. Section **13-61-303** is enacted to read:

13-61-303. Processing deidentified data or pseudonymous data.

(1) The provisions of this chapter do not require a controller or processor to:

(a) reidentify deidentified data or pseudonymous data;

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

(c) comply with an authenticated consumer request to exercise a right described in Subsections 13-61-202(1) through (3), if:

(i) (A) the controller is not reasonably capable of associating the request with the personal data; or

(B) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) the controller does not:

(A) use the personal data to recognize or respond to the consumer who is the subject of the personal data; or

(B) associate the personal data with other personal data about the consumer; and

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

(2) The rights described in Subsections 13-61-201(1) through (3) do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept:

(a) separately; and

(b) subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.

(3) A controller who uses pseudonymous data or deidentified data shall take reasonable steps to ensure the controller:

(a) complies with any contractual obligations to which the pseudonymous data or deidentified data are subject; and

(b) promptly addresses any breach of a contractual obligation described in Subsection (3)(a).

Section 11. Section **13-61-304** is enacted to read:

13-61-304. Limitations.

(1) The requirements described in this chapter do not restrict a controller or processor's ability to:

(a) comply with a federal, state, or local law, rule, or regulation;

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

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

(d) investigate, establish, exercise, prepare for, or defend a legal claim;

(e) provide a product or service requested by a consumer or a parent or legal guardian of a child;

(f) perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian before entering into the contract with the consumer;

(g) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual;

(h) (i) detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or

(ii) investigate, report, or prosecute a person responsible for an action described in Subsection (1)(h)(i);

(i) (i) preserve the integrity or security of systems; or

(ii) investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable;

(j) if the controller discloses the processing in a notice described in Section 13-61-302, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws;

(k) assist another person with an obligation described in this subsection;

(l) process personal data to:

(i) conduct internal analytics or other research to develop, improve, or repair a controller or processor's product, service, or technology;

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

(iii) effectuate a product recall;

(m) process personal data to perform an internal operation that is:

(i) reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller; or

(ii) otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party; or

(n) retain a consumer's email address to comply with the consumer's request to exercise a right.

(2) This chapter does not apply if a controller or processor's compliance with this chapter:

(a) violates an evidentiary privilege under Utah law;

(b) as part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Utah law; or

(c) adversely affect the privacy or other rights of any person.

(3) A controller or processor is not in violation of this chapter if:

(a) the controller or processor discloses personal data to a third party controller or processor in compliance with this chapter;

(b) the third party processes the personal data in violation of this chapter; and

(c) the disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this chapter.

(4) If a controller processes personal data under an exemption described in Subsection (1), the controller bears the burden of demonstrating that the processing qualifies for the exemption.

(5) Nothing in this chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

Section 12. Section **13-61-305** is enacted to read:

13-61-305. No private cause of action.

A violation of this chapter does not provide a basis for, nor is a violation of this chapter subject to, a private right of action under this chapter or any other law.

Section 13. Section **13-61-401** is enacted to read:

Part 4. Enforcement

13-61-401. Investigative powers of division.

(1) The division shall establish and administer a system to receive consumer complaints regarding a controller or processor's alleged violation of this chapter.

(2) (a) The division may investigate a consumer complaint to determine whether the controller or processor violated or is violating this chapter.

(b) If the director has reasonable cause to believe that substantial evidence exists that a person identified in a consumer complaint is in violation of this chapter, the director shall refer the matter to the attorney general.

(c) Upon request, the division shall provide consultation and assistance to the attorney general in enforcing this chapter.

Section 14. Section **13-61-402** is enacted to read:

13-61-402. Enforcement powers of the attorney general.

(1) The attorney general has the exclusive authority to enforce this chapter.

(2) Upon referral from the division, the attorney general may initiate an enforcement action against a controller or processor for a violation of this chapter.

(3) (a) At least 30 days before the day on which the attorney general initiates an enforcement action against a controller or processor, the attorney general shall provide the controller or processor:

(i) written notice identifying each provision of this chapter the attorney general alleges the controller or processor has violated or is violating; and

(ii) an explanation of the basis for each allegation.

(b) The attorney general may not initiate an action if the controller or processor:

(i) cures the noticed violation within 30 days after the day on which the controller or processor receives the written notice described in Subsection (3)(a); and

(ii) provides the attorney general an express written statement that:

(A) the violation has been cured; and

(B) no further violation of the cured violation will occur.

(c) The attorney general may initiate an action against a controller or processor who:

(i) fails to cure a violation after receiving the notice described in Subsection (3)(a); or

(ii) after curing a noticed violation and providing a written statement in accordance with Subsection (3)(b), continues to violate this chapter.

(d) In an action described in Subsection (3)(c), the attorney general may recover:

(i) actual damages to the consumer; and

(ii) for each violation described in Subsection (3)(c), an amount not to exceed $7,500.

(4) All money received from an action under this chapter shall be deposited into the Consumer Privacy Account established in Section 13-61-403.

(5) If more than one controller or processor are involved in the same processing in violation of this chapter, the liability for the violation shall be allocated among the controllers or processors according to the principles of comparative fault.

Section 15. Section **13-61-403** is enacted to read:

13-61-403. Consumer Privacy Restricted Account.

(1) There is created a restricted account known as the "Consumer Privacy Account."

(2) The account shall be funded by money received through civil enforcement actions under this chapter.

(3) Upon appropriation, the division or the attorney general may use money deposited into the account for:

(a) investigation and administrative costs incurred by the division in investigating consumer complaints alleging violations of this chapter;

(b) recovery of costs and attorney fees accrued by the attorney general in enforcing this chapter; and

(c) providing consumer and business education regarding:

(i) consumer rights under this chapter; and

(ii) compliance with the provisions of this chapter for controllers and processors.

(4) If the balance in the account exceeds $4,000,000 at the close of any fiscal year, the Division of Finance shall transfer the amount that exceeds $4,000,000 into the General Fund.

Section 16. Section **13-61-404** is enacted to read:

13-61-404. Attorney general report.

(1) The attorney general and the division shall compile a report:

(a) evaluating the liability and enforcement provisions of this chapter, including the effectiveness of the attorney general's and the division's efforts to enforce this chapter; and

(b) summarizing the data protected and not protected by this chapter including, with reasonable detail, a list of the types of information that are publicly available from local, state, and federal government sources.

(2) The attorney general and the division may update the report as new information becomes available.

(3) The attorney general and the division shall submit the report to the Business and Labor Interim Committee before July 1, 2025.

Section 17. **Effective date.**

This bill takes effect on December 31, 2023.