A bill

TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ADDING CHAPTER 31 TO TITLE 37 SO AS TO PROVIDE DEFINITIONS, TO PROVIDE THAT A GOVERNMENTAL ENTITY MAY NOT COMMUNICATE WITH A SOCIAL MEDIA PLATFORM IN CERTAIN INSTANCES, TO PROVIDE APPLICABILITY, TO PROVIDE EXEMPTIONS, TO PROVIDE FOR CERTAIN CONSUMER RIGHTS, TO PROVIDE FOR THE EXERCISING OF CERTAIN RIGHTS, TO ESTABLISH AN APPEALS PROCESS, TO PROVIDE THAT CERTAIN CONTRACTS AND AGREEMENTS THAT WAIVE RIGHTS ARE VOID, TO PROVIDE THAT A CONTROLLER SHALL ESTABLISH METHODS TO SUBMIT REQUESTS, TO PROVIDE FOR DUTIES FOR CONTROLLERS, TO PROVIDE FOR A PRIVACY NOTICE, TO PROVIDE FOR DUTIES OF A PROCESSOR, TO PROVIDE FOR A DATA PROTECTION ASSESSMENT, TO PROVIDE FOR DUTIES OF A CONTROLLER IN POSSESSION OF DEIDENTIFIED DATA, TO PROVIDE THAT A CONTROLLER MAY NOT ENGAGE IN THE SALE OF CERTAIN PERSONAL DATA, TO PROVIDE FOR ACTIONS THAT ARE NOT RESTRICTED, TO PROVIDE FOR THIRD‑PARTY DATA DISCLOSURE, TO PROVIDE THAT CERTAIN PERSONAL DATA MAY NOT BE PROCESSED, AND TO PROVIDE THAT A VIOLATION IS AN UNFAIR AND DECEPTIVE TRADE PRACTICE.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. Title 37 of the S.C. Code is amended by adding:

CHAPTER 31

Technology Transparency

Section 37-31-100. As used in this chapter:

(1) “Affiliate” means a legal entity that controls, is controlled by, or is under common control with another legal entity or that shares common branding with another legal entity. For purposes of this item, the term “control” or “controlled” means any of the following:

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

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

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

(2) “Aggregate consumer information” means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with any consumer, household, or device. The term does not include information about a group or category of consumers used to facilitate targeted advertising or the display of ads online. The term does not include personal information that has been deidentified.

(3) “Authenticate” or “authenticated” means to verify or the state of having been verified, respectively, through reasonable means that the consumer who is entitled to exercise the consumer’s rights pursuant to this chapter is the same consumer exercising those consumer rights with respect to the personal data at issue.

(4) “Biometric data” means data generated by automatic measurements of an individual’s biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996.

(5) “Business associate” has the same meaning as in 45 C.F.R. Section 160.103 and the Health Insurance Portability and Accountability Act of 1996.

(6) “Child” means an individual younger than eighteen years of age.

(7) “Consent”, when referring to a consumer, means a clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act. The term does not include any of the following:

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

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

(c) agreement obtained through the use of dark patterns.

(8) “Consumer” means an individual who is a resident of or is domiciled in this State acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(9) “Controller” means:

(a) a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

(i) is organized or operated for the profit or financial benefit of its shareholders or owners;

(ii) conducts business in this State;

(iii) collects personal data about consumers or is the entity on behalf of which the information is collected;

(iv) determines the purposes and means of processing personal data about consumers alone or jointly with others;

(v) makes in excess of one billion dollars in global gross annual revenues; and

(vi) satisfies at least one of the following:

(A) derives fifty percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;

(B) operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands‑free verbal activation. For purposes of this subsubsubitem, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or

(C) operates an app store or a digital distribution platform that offers at least two hundred fifty thousand different software applications for consumers to download and install; or

(b) any entity that controls or is controlled by a controller. As used in this subitem, the term “control” means:

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

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

(iii) the power to exercise a controlling influence over the management of a company.

(10) “Covered entity” has the same meaning as in 45 C.F.R. Section 160.103 and the Health Insurance Portability and Accountability Act of 1996.

(11) “Dark pattern” means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision making, or choice. The term includes any practice the Federal Trade Commission refers to as a dark pattern.

(12) “Decision that produces a legal or similarly significant effect concerning a consumer” means a decision made by a controller which results in the provision or denial by the controller of any of the following:

(a) financial and lending services;

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

(c) education enrollment;

(d) employment opportunities;

(e) criminal justice; or

(f) access to basic necessities, such as food and water.

(13) “Deidentified data” means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.

(14) “Governmental entity” means any state, county, district, authority, or municipal office, department, division, board, bureau, commission, or other separate unit of government created or established by law and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

(15) “Health care provider” has the same meaning as in 45 C.F.R. Section 160.103 and the Health Insurance Portability and Accountability Act of 1996.

(16) “Health record” means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual which concerns the individual and the services provided. The term includes any of the following:

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

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

(17) “Identified or identifiable individual” means a consumer who can be readily identified, directly or indirectly.

(18) “Known child” means a child under circumstances of which a controller has actual knowledge of, or wilfully disregards, the child’s age.

(19) “Nonprofit organization” means any of the following:

(a) an organization exempt from federal taxation under Section 501(a) of the Internal Revenue Code of 1986 by virtue of being listed as an exempt organization under Section 501(c)(3), 501(c)(4), 501(c)(6), or 501(c)(12) of that code; or

(b) a political organization.

(20) “Personal data” means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(21) “Personal information” means either:

(a) an individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(i) a social security number;

(ii) a driver’s license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(iii) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;

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

(v) an individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;

(vi) an individual’s biometric data as defined in this chapter; or

(vii) any information regarding an individual’s geolocation; or

(b) a username or email address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(22) “Political organization” means a party, a committee, an association, a fund, or any other organization, regardless of whether incorporated, organized, and operated primarily for the purpose of influencing or attempting to influence any of the following:

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

(b) the election of a presidential or vice‑presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.

(23) “Postsecondary education institution” means a state university or nonpublic postsecondary education institution that receives state funds.

(24) “Precise geolocation data” means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

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

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

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

(28) “Protected health information” has the same meaning as in 45 C.F.R. Section 160.103 and the Health Insurance Portability and Accountability Act of 1996.

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

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

(31) “Sale of personal data” means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:

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

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

(c) the disclosure of information that the consumer:

(i) intentionally made available to the general public through a mass media channel; and

(ii) did not restrict to a specific audience; or

(d) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition.

(32) “Search engine” means technology and systems that use algorithms to sift through and index vast third‑party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third‑party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.

(33) “Sensitive data” means a category of personal data which includes any of the following:

(a) personal data revealing an individual’s racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

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

(c) personal data collected from a known child; and

(d) precise geolocation data.

(34) “Social media platform” means a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.

(35) “State agency” means any department, commission, board, office, council, authority, or other agency in the executive branch of state government created by the State Constitution or state law. The term includes a postsecondary education institution.

(36) “Targeted advertising” means displaying to a consumer an advertisement selected based on personal data obtained from that consumer’s activities over time and across nonaffiliated websites or online applications to predict the consumer’s preferences or interests. The term does not include any of the following:

(a) an advertisement that is:

(i) based on activities within a controller’s own website or online application;

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

(iii) directed to a consumer in response to the consumer’s request for information or feedback; or

(b) the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

(37) “Third party” means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.

(38) “Trade secret” means a secret device or technique used by a company in manufacturing its products.

(39) “Voice recognition feature” means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

Section 37-31-110. (A) An officer or a salaried employee of a governmental entity may not use his position or any state resources to communicate with a social media platform to request the social media platform to remove content or accounts from the social media platform.

(B) A governmental entity, or an officer or a salaried employee acting on behalf of a governmental entity, may not initiate or maintain any agreements or working relationships with a social media platform for the purpose of content moderation.

(C) Subsections (A) and (B) do not apply if the governmental entity or an officer or a salaried employee acting on behalf of a governmental entity is acting as part of any of the following:

(1) routine account management of the governmental entity’s account including, but not limited to, the removal or revision of the governmental entity’s content or account or identification of accounts falsely posing as a governmental entity, officer, or salaried employee;

(2) an attempt to remove content that pertains to the commission of a crime or violation of this state’s public records law;

(3) an attempt to remove an account that pertains to the commission of a crime or violation of this state’s public records law; or

(4) an investigation or inquiry related to an effort to prevent imminent bodily harm, loss of life, or property damage.

Section 37-31-120. (A) This chapter applies only to a person who:

(1) conducts business in this State or produces a product or service used by residents of this State; and

(2) processes or engages in the sale of personal data.

(B) This chapter does not apply to:

(1) a state agency or a political subdivision of the State;

(2) a financial institution or data subject to Title V, Gramm‑Leach‑Bliley Act;

(3) a covered entity or business associate governed by the privacy, security, and breach notification regulations issued by the United States Department of Health and Human Services, established under the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII and Division B, Title IV, Pub. L. No. 111‑5;

(4) a nonprofit organization; or

(5) a postsecondary educational institution.

(C) This chapter does not apply to the processing of personal data by a person in the course of a purely personal or household activity.

(D) A controller or processor that complies with the authenticated parental consent requirements of the Children’s Online Privacy Protection Act with respect to data collected online is considered to be in compliance with any requirement to obtain parental consent pursuant to this chapter.

Section 37-31-130. All of the following information is exempt from this chapter:

(1) protected health information pursuant to the Health Insurance Portability and Accountability Act of 1996;

(2) health records;

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

(4) identifiable private information:

(a) for purposes of the federal policy for the protection of human subjects under 45 C.F.R. part 46;

(b) collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects pursuant to 21 C.F.R. parts 50 and 56; or

(c) that is personal data used or shared in research conducted in accordance with this chapter or other research conducted in accordance with applicable law;

(5) information and documents created for purposes of the Health Care Quality Improvement Act of 1986;

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

(7) information derived from any of the health care‑related information listed in this section which is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996;

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

(9) information included in a limited data set as described by 45 C.F.R. Section 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. Section 164.514(e);

(10) information used only for public health activities and purposes as described in 45 C.F.R. Section 164.512;

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

(12) the collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act;

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

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

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

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

(17) data processed or maintained as the emergency contact information of an individual pursuant to this chapter which is used for emergency contact purposes;

(18) data that is processed or maintained and that is necessary to retain to administer benefits for another individual which relates to an individual described in item (16) and which is used for the purposes of administering those benefits;

(19) personal data collected and transmitted which is necessary for the sole purpose of sharing the personal data with a financial service provider solely to facilitate short‑term, transactional payment processing for the purchase of products or services;

(20) personal data collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the Airline Deregulation Act by entities subject to that act, to the extent the provisions of this chapter are preempted by 49 U.S.C. Section 41713; and

(21) personal data shared between a manufacturer of a tangible product and authorized third‑party distributors or vendors of the product, as long as the personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through the manufacturer and the authorized third‑party distributors or vendors. The personal data may not be sold or shared unless otherwise authorized pursuant to this chapter.

Section 37-31-140. (A) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child.

(B) A controller shall comply with an authenticated consumer request to exercise any of the following rights:

(1) to confirm whether a controller is processing the consumer’s personal data and to access the personal data.

(2) to 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) to delete any or all personal data provided by or obtained about the consumer;

(4) to obtain a copy of the consumer’s personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format;

(5) to opt out of the processing of the personal data for purposes of:

(a) targeted advertising;

(b) the sale of personal data; or

(c) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer;

(6) to opt out of the collection of sensitive data, including precise geolocation data or the processing of such data; or

(7) to opt out of the collection of personal data collected through the operation of a voice recognition feature.

Section 37-31-150. (A) Except as otherwise provided by this chapter, a controller shall comply with a request submitted by a consumer to exercise the consumer’s rights pursuant to Section 37‑31‑140, as provided in this section.

(B) A controller shall respond to the consumer request without undue delay, which may not be later than forty‑five days after the date of receipt of the request. The controller may extend the response period once by an additional fifteen days when reasonably necessary, taking into account the complexity and number of the consumer’s requests, so long as the controller informs the consumer of the extension within the initial forty‑five‑day response period, together with the reason for the extension.

(C) If a controller cannot take action regarding the consumer’s request, the controller must inform the consumer without undue delay, which may not be later than forty‑five days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision in accordance with Section 37‑31‑160. A controller is not required to comply with a consumer request submitted under Section 37‑31‑140 if the controller cannot authenticate the request. However, the controller must make a reasonable effort to request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer’s request. If a controller maintains a self‑service mechanism to allow a consumer to correct certain personal data, the controller may deny the consumer’s request and require the consumer to correct his own personal data through such mechanism.

(D) A controller shall provide the consumer with notice within sixty days after the request is received that the controller has complied with the consumer’s request as required in this section.

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

(F) A controller who has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer’s request to delete that personal data pursuant to Section 37‑31‑140, by doing any of the following:

(1) deleting the personal data, retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer’s personal data remains deleted from the business’s records and not using the retained data for any other purpose pursuant to this chapter; or

(2) opting the consumer out of the processing of that personal data for any purpose other than a purpose exempt pursuant to this chapter.

Section 37-31-160. (A) 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 Section 37‑31‑150.

(B) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request pursuant to Section 37‑31‑140.

(C) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal pursuant to this section within sixty days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

Section 37-31-170. Any provision of a contract or agreement which waives or limits in any way a consumer right described by Sections 37‑31‑140 through 37‑31‑160 is contrary to public policy and is void and unenforceable.

Section 37-31-180. (A) A controller shall establish two or more methods to enable consumers to submit a request to exercise their consumer rights pursuant to this chapter. The methods must be secure, reliable, and clearly and conspicuously accessible. The methods must take all of the following into account:

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

(2) the necessity for secure and reliable communications of these requests; and

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

(B) A controller may not require a consumer to create a new account to exercise the consumer’s rights pursuant to this chapter but may require a consumer to use an existing account.

(C) A controller shall provide a mechanism on its website for a consumer to submit a request for information required to be disclosed pursuant to this chapter. A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal data also may provide an email address for the submission of requests.

Section 37-31-190. (A) A controller shall:

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

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

(B) A controller may not:

(1) except as otherwise provided by this chapter, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer’s consent;

(2) process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers;

(3) discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that the incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time; or

(4) process the sensitive data of a consumer without obtaining the consumer’s consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for the processing by a known child who is between thirteen and eighteen years of age or in accordance with the Children’s Online Privacy Protection Act for a known child under the age of thirteen.

(C) Subsection (B)(3) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer which 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 37‑31‑140 or the offer is related to a consumer’s voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(D) A controller that operates a search engine shall make available, in an easily accessible location on the webpage which does not require a consumer to log in or register to read, an up‑to‑date plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers through the manipulation of search results.

Section 37-31-200. (A) A controller shall provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:

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

(2) the purpose of processing personal data;

(3) how consumers may exercise their rights pursuant to Section 37‑31‑140, including the process by which a consumer may appeal a controller’s decision with regard to the consumer’s request;

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

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

(6) a description of the methods specified in Section 37‑31‑180, by which consumers can submit requests to exercise their consumer rights pursuant to this chapter.

(B) If a controller engages in the sale of personal data that is sensitive data, the controller shall provide the following notice: “NOTICE: This website may sell your sensitive personal data.” The notice must be posted in accordance with subsection (A).

(C) If a controller engages in the sale of personal data that is biometric data, the controller shall provide the following notice: “NOTICE: This website may sell your biometric personal data.” The notice must be posted in accordance with subsection (A).

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

(E) A controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

Section 37-31-210. (A) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller’s duties pursuant to this section and the requirements of this chapter, including:

(1) assisting the controller in responding to consumer rights requests submitted pursuant to Sections 37‑31‑140 and 37‑31‑180, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor;

(2) assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor’s system taking into account the nature of processing and the information available to the processor; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments pursuant to Section 37‑31‑220.

(B) A contract between a controller and a processor governs the processor’s data processing procedures with respect to processing performed on behalf of the controller. The contract must include:

(1) clear instructions for processing data;

(2) the nature and purpose of processing;

(3) the type of data subject to processing;

(4) the duration of processing;

(5) the rights and obligations of both parties;

(6) a requirement that the processor:

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

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

(c) make available to the controller, upon reasonable request, all information in the processor’s possession necessary to demonstrate the processor’s compliance with this chapter;

(d) allow, and cooperate with, reasonable assessments by the controller or the controller’s designated assessor; and

(e) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

(C) Notwithstanding subsection (B)(6)(d), a 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 requirements pursuant to this chapter using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller upon request.

(D) This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this chapter.

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

Section 37-31-220. (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 if the 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 on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

(d) other substantial injury to consumers;

(4) the processing of sensitive data; and

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

(B) A data protection assessment conducted pursuant to subsection (A) must:

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

(2) factor into the assessment:

(a) the use of deidentified data;

(b) the reasonable expectations of consumers;

(c) the context of the processing; and

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

(C) The disclosure of a data protection assessment in compliance with a request from the Attorney General does not constitute a waiver of attorney‑client privilege or work product protection with respect to the assessment and any information contained in the assessment.

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

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

(F) This section applies only to processing activities generated after June 30, 2025.

Section 37-31-230. (A) A controller in possession of deidentified data shall:

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

(2) maintain and use the data in deidentified form. A controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section;

(3) contractually obligate any recipient of the deidentified data to comply with this chapter; and

(4) implement business processes to prevent the inadvertent release of deidentified data.

(B) This chapter may not be construed to require a controller or processor to do any of the following:

(1) reidentify deidentified data or pseudonymous data;

(2) maintain data in an 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;

(3) comply with an authenticated consumer rights request pursuant to Section 37‑31‑140 if the controller:

(a) 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;

(b) 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

(c) 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 authorized by this section.

(C) The consumer rights enumerated pursuant to Section 37‑31‑140 and controller duties do not apply to pseudonymous data or aggregate consumer information in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separate and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

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

Section 37-31-240. (A) A person who meets the requirements for the definition of a controller may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer or, if the sensitive data is of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between thirteen and eighteen years of age or in accordance with the Children’s Online Privacy Protection Act for a known child under the age of thirteen.

(B) A person who engages in the sale of personal data that is sensitive data, pursuant to subsection (A), shall provide the following notice: “NOTICE: This website may sell your sensitive personal data.”

(C) A person who violates this section is subject to the penalty imposed pursuant to Section 37‑31‑290.

Section 37-31-250. (A) This chapter may not be construed to restrict a controller’s or processor’s ability to do any of the following:

(1) comply with federal or state laws, rules, or regulations;

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

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

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

(5) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;

(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 or investigate, report, or prosecute those responsible for breaches of system security;

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

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

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

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

(9) assist another controller, processor, or third party in complying with the requirements of this chapter;

(10) disclose personal data disclosed when a consumer uses or directs the controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party; or

(11) transfer personal data to a third party as an asset that is part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in a manner consistent with this chapter. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this chapter.

(B) This chapter may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this State as part of a privileged communication.

(C) This chapter may not be construed as imposing a requirement on controllers and processors which adversely affects the rights or freedoms of any person, including the right of free speech.

(D) This chapter may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.

Section 37-31-260. (A) The requirements imposed on controllers and processors pursuant to this chapter may 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) effect a product recall;

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

(4) perform internal operations that are:

(a) reasonably aligned with the expectations of the consumer;

(b) reasonably anticipated based on the consumer’s existing relationship with the controller; or

(c) 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.

(B) A requirement imposed on a controller or processor pursuant to this chapter does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege pursuant to the laws of this State.

Section 37-31-270. (A) A controller or processor that discloses personal data to a third‑party controller or processor in compliance with the requirements of this chapter does not violate this chapter if the third‑party controller or processor that receives and processes that personal data violates this chapter, provided that, at the time of the data’s disclosure, the disclosing controller or processor could not have reasonably known that the recipient intended to commit a violation.

(B) A third‑party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter may not be held liable for violations of this chapter committed by the controller or processor from which the third‑party controller or processor receives the personal data.

Section 37-31-280. (A) Personal data processed by a controller pursuant to Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270 may not be processed for any purpose other than those specified in those sections. Personal data processed by a controller pursuant to Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270 may be processed to the extent that the processing of the data is:

(1) reasonably necessary and proportionate to the purposes specified in Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270;

(2) adequate, relevant, and limited to what is necessary in relation to the purposes specified in Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270; and

(3) done to assist another controller, processor, or third party with any of the purposes specified in Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270.

(B) A controller or processor that collects, uses, or retains personal data for the purposes specified in Section 37‑31‑260 must take into account the nature and purpose of the collection, use, or retention. The personal data is subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(C) A controller or processor shall adopt and implement a retention schedule that prohibits the use or retention of personal data not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which the information was collected or obtained, after the expiration or termination of the contract pursuant to which the information was collected or obtained, or two years after the consumer’s last interaction with the controller or processor. This subsection does not apply to personal data reasonably used or retained to:

(1) provide a good or service requested by the consumer, or reasonably anticipate the request of a good or service within the context of a controller’s ongoing business relationship with the consumer;

(2) debug to identify and repair errors that impair existing intended functionality; or

(3) enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the controller or that are compatible with the context in which the consumer provided the information.

(D) A controller or processor that processes personal data pursuant to Sections 37‑31‑250, 37‑31‑260, and 37‑31‑270 bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of this section.

Section 37-31-290. (A) A violation of this chapter is an unfair and deceptive trade practice actionable as provided by law. If the Attorney General has reason to believe that a person is in violation of this chapter, the Office of Attorney General may, as the enforcing authority, bring an action against such person for an unfair or deceptive act or practice. The Office of Attorney General may collect a civil penalty of up to fifty thousand dollars for each violation. Civil penalties may be tripled for:

(1) a violation involving a South Carolina consumer who is a known child. A controller that wilfully disregards the consumer’s age is considered to have actual knowledge of the consumer’s age;

(2) failure to delete or correct the consumer’s personal data pursuant to this chapter after receiving an authenticated consumer request or directions from a controller to delete or correct the personal data, unless an exception to the requirements to delete or correct the personal data pursuant to this chapter applies; or

(3) continuing to sell or share the consumer’s personal data after the consumer chooses to opt out pursuant to this chapter.

(B) After the Attorney General has notified a person in writing of an alleged violation, the Attorney General may grant a forty‑five‑day period to cure the alleged violation and issue a letter of guidance. The forty‑five‑day cure period does not apply to an alleged violation of subsection (A)(1). The Attorney General may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property in determining whether to grant forty‑five calendar days to cure and the issuance of a letter of guidance. If the alleged violation is cured to the satisfaction of the Attorney General and proof of the cure is provided to the Attorney General, the Attorney General may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the person will not be offered a forty‑five‑day cure period for any future violations. If the person fails to cure the alleged violation within forty‑five calendar days, the Attorney General may bring an action against the person for the alleged violation.

(C) Any action brought by the Attorney General may be brought only on behalf of a South Carolina consumer.

(D) By February first of each year, the Office of Attorney General shall make a report publicly available on the office’s website describing any actions taken by the office to enforce this section. The report must include statistics and relevant information detailing:

(1) the number of complaints received and the categories or types of violations alleged by the complainant;

(2) the number and type of enforcement actions taken and the outcomes of the actions, including the amount of penalties issued and collected;

(3) the number of complaints resolved without the need for litigation; and

(4) for the report due February 1, 2025, the status of the development and implementation of rules to implement this section.

(E) The Office of Attorney General shall adopt rules to implement this section, including standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer’s behalf.

(F) The Office of Attorney General may collaborate and cooperate with other enforcement authorities of the federal government or other state governments concerning consumer data privacy issues and consumer data privacy investigations if the enforcement authorities have restrictions governing confidentiality at least as stringent as the restrictions provided in this section.

(G) Liability for a tort, contract claim, or consumer protection claim unrelated to an action brought pursuant to this section does not arise solely from the failure of a person to comply with this chapter.

(H) This chapter does not establish a private cause of action.

(I) The Office of Attorney General may employ or use the legal services of outside counsel and the investigative services of outside personnel to fulfill the obligations of this section.

(J) For purposes of bringing an action pursuant to this section, any person who meets the definition of controller as defined in this chapter who collects, shares, or sells the personal data of South Carolina consumers is considered to be engaged in both substantial and not isolated activities within this State and operating, conducting, engaging in, or carrying on a business, and doing business in this State, and is, therefore, subject to the jurisdiction of the courts of this State.

SECTION 2. This act takes effect upon approval by the Governor.

‑‑‑‑XX‑‑‑‑