**South Carolina General Assembly**

125th Session, 2023-2024

**H. 4842**

**STATUS INFORMATION**

General Bill

Sponsors: Rep. Guffey

Document Path: LC-0442SA24.docx

Introduced in the House on January 16, 2024

Currently residing in the House Committee on **Judiciary**

Summary: Age-Appropriate Design

**HISTORY OF LEGISLATIVE ACTIONS**

 Date Body Action Description with journal page number

 1/16/2024 House Introduced and read first time (House Journal‑page 9)

 1/16/2024 House Referred to Committee on **Judiciary** (House Journal‑page 9)

View the latest  [legislative information](https://www.scstatehouse.gov/billsearch.php?billnumbers=4842&session=125&summary=B)  at the website

**VERSIONS OF THIS BILL**

[01/16/2024](https://www.scstatehouse.gov/sess125_2023-2024/prever/4842_20240116.docx)

A bill

TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ADDING CHAPTER 79 TO TITLE 39 BY ENACTING THE “SOUTH CAROLINA AGE‑APPROPRIATE DESIGN CODE ACT” SO AS TO PROVIDE DEFINITIONS, TO PROVIDE FOR INFORMATION FIDUCIARY, TO PROVIDE SCOPE AND EXCLUSIONS, TO PROVIDE REQUIREMENTS FOR COVERED ENTITIES, TO PROVIDE FOR PROHIBITIONS FOR COVERED ENTITIES, TO PROVIDE FOR DATA PRACTICES, TO PROVIDE FOR ENFORCEMENT, AND TO PROVIDE FOR LIMITATIONS.

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

SECTION 1. This act may be cited as the “South Carolina Age‑Appropriate Design Code Act”.

SECTION 2. Title 39 of the S.C. Code is amended by adding:

CHAPTER 79

Age‑Appropriate Design Code

 Section 39‑79‑10. As used in this chapter:

 (1) “Affiliate” means legal entity that controls, is controlled by, or is under common control with, that other legal entity. For these purposes, “control” or “controlled” means ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a covered entity, control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or the power to exercise a controlling influence over the management of a covered entity.

 (2) “Age‑appropriate” means a recognition of the distinct needs and diversities of children at different age ranges. To help support the design of online services, products, and features, covered entities should take into account the unique needs and diversities of different age ranges, including the following developmental stages: zero to five years of age or “preliterate and early literacy”; six to nine years of age or “core primary school years”; ten to twelve years of age or “transition years”; thirteen to fifteen years of age or “early teens”; and sixteen to seventeen years or age or “approaching adulthood.”

 (3) “Best interests of children” means the use, by a covered entity, of the personal data of a child or the design of an online service, product, or feature in a way that:

 (a) will not benefit the covered entity to the detriment of the child; and

 (b) will not result in:

 (i) reasonably foreseeable and material, physical, or financial harm to the child;

 (ii) reasonably foreseeable and severe psychological or emotional harm to the child;

 (iii) a highly offensive intrusion on the reasonable privacy expectations of the child; or

 (iv) discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation.

 (4) “Child” means a consumer who is under eighteen years of age.

 (5) “Collect” means buying, renting, gathering, obtaining, receiving, or accessing any personal data pertaining to a consumer by any means. This includes receiving data from the consumer, either actively or passively, or by observing the consumer’s behavior.

 (6)(a) “Covered entity” means:

 (i) a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners; and

 (ii) an affiliate of a covered entity that shares common branding with the covered entity. For purposes of this subsubitem, “common branding” means a shared name, service mark, or trademark that the average consumer would understand that two or more entities are commonly owned.

 (b) For purposes of this chapter, for a joint venture or partnership composed of covered entities in which each covered entity has at least a forty percent interest, the joint venture or partnership and each covered entity that composes the joint venture or partnership must be separately considered a single covered entity, except that personal data in the possession of each covered entity and disclosed to the joint venture or partnership may not be shared with the other covered entity.

 (7) “Consumer” means a natural person who is a South Carolina resident, however identified, including by any unique identifier.

 (8) “Dark pattern” means a user interface designed or manipulated with the purpose of subverting or impairing user autonomy, decision making, or choice.

 (9) “Data protection impact assessment” means a systematic survey to assess compliance with the duty to act in the best interests of children and includes a plan to ensure that all online products, services, or features provided by the covered entity are designed and offered in a manner consistent with the best interests of children reasonably likely to access the online product, service, or feature. Such a plan must include a description of steps the covered entity has taken and will take to comply with the duty to act in the best interests of children.

 (10) “Default” means a preselected option adopted by the covered entity for the online service, product, or feature.

 (11) “Deidentified” means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the covered entity that possesses the data:

 (a) takes reasonable measures to ensure that the data cannot be associated with a natural person;

 (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and

 (c) contractually obligates any recipients of the data to comply with all provisions of this item.

 (12) “Derived data” means data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about a child or a child’s device.

 (13) “Online service, product, or feature” does not mean any of the following:

 (a) a telecommunications service, as defined in 47 U.S.C. Section 153;

 (b) a broadband service as defined by Sections 58‑9‑10 (17) and 58‑9‑3010 (5); or

 (c) the sale, delivery, or use of a physical product.

 (14) “Personal data” means any information, including derived data, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information. For purposes of this item, “publicly available information” means information that is lawfully made available from federal, state, or local government records or widely distributed media, and a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

 (15) “Precise geolocation” means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand eight hundred fifty feet, except as prescribed by regulations.

 (16) “Product experimentation results” means the data that companies collect to understand the experimental impact of their products.

 (17) “Process” or “processing” means to conduct or direct any 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, modification, or otherwise handling of personal data.

 (18) “Profiling” means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. “Profiling” does not include the processing of information that does not result in an assessment or judgment about a natural person.

 (19) “Reasonably likely to be accessed” means an online service, product, or feature that is accessed by children based on any of the following indicators:

 (a) the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, 15 U.S.C. Section 6501 et seq., and the Federal Trade Commission rules implementing that act;

 (b) the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;

 (c) the online service, product, or feature contains advertisements marketed to children;

 (d) the online service, product, or feature is substantially similar or the same as an online service, product, or feature subject to subitem (b);

 (e) a significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children; or

 (f) the covered entity knew or should have known that a significant number of users are children, provided that, in making this assessment, the covered entity may not collect or process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged.

 (20) “Sale”, “sell”, or “sold” means the exchange of personal data for monetary or other valuable consideration by a covered entity to a third party. Sale does not include:

 (a) the disclosure of personal data to a third party who processes the personal data on behalf of the covered entity;

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

 (c) the disclosure or transfer of personal data to an affiliate of the covered entity;

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

 (e) the disclosure or transfer of personal data to a third party as an asset that is part of a completed or proposed merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the covered entity’s assets.

 (21) “Share” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means a consumer’s personal data by the covered entity to a third party for cross‑context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a covered entity and a third party for cross‑context behavioral advertising for the benefit of a covered entity in which no money is exchanged.

 (22) “Third party” means a natural or legal person, public authority, agency, or body other than the consumer or the covered entity.

 Section 39‑79‑20. All covered entities that operate in this State and process children’s data in any capacity must do so in a manner consistent with the best interests of children.

 Section 39‑79‑30. (A) A covered entity is subject to the requirements of this chapter other than Section 39‑79‑20 if it:

 (1) collects consumers’ personal data or has consumers’ personal data collected on its behalf by a third party;

 (2) alone or jointly with others, determines the purposes and means of the processing of consumers’ personal data;

 (3) operates in South Carolina; and

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

 (i) has annual gross revenues more than twenty‑five million dollars, as adjusted every odd‑numbered year to reflect the Consumer Price Index;

 (ii) alone or in combination, annually buys, receives for the covered entity’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of fifty thousand or more consumers, households, or devices; or

 (iii) derives fifty percent or more of its annual revenues from selling consumers’ personal data.

 (B) This chapter does not apply to:

 (1) protected health information that is collected by a covered entity or covered entity associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Code of Federal Regulations, Title 45, Parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Public Law 104‑191, and the Health Information Technology for Economic and Clinical Health Act, Public Law 111‑5;

 (2) a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Code of Federal Regulations, Title 45, Parts 160 and 164, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Public Law 104‑191, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in item (1); or

 (3) information collected as part of a clinical trial subject to the federal policy for the protection of human subjects, also known as the common rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

 Section 39‑79‑40. (A) A covered entity subject to this chapter shall:

 (1) complete a data protection impact assessment for that online service, product, or feature, and any new online service, product, or feature that is reasonably likely to be to accessed by children, and maintain documentation of the data protection impact assessment for as long as the online service, product, or feature is reasonably likely to be accessed by children;

 (2) review and modify all data protection impact assessments as necessary to account for material changes to processing pertaining to the online service, product, or feature within ninety days of such material changes;

 (3) within five business days of a written request by the Attorney General, provide to the Attorney General a list of all data protection impact assessments the covered entity has completed;

 (4) within five business days of a written request by the Attorney General, provide the Attorney General with a copy of any data protection impact assessment. The Attorney General may, in his discretion, extend beyond seven business days the amount of time allowed for a covered entity to produce a data protection impact assessment;

 (5) configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the covered entity can demonstrate a compelling reason that a different setting is in the best interests of children;

 (6) provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children reasonably likely to access that online service, product, or feature; and

 (7) provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

 (B) A data protection impact assessment required by this section must identify the purpose of the online service, product, or feature; how it uses children’s personal data; and determine whether the online service, product, or feature is designed and offered in an age‑appropriate manner consistent with the best interests of children that are reasonably likely to access the online product by examining at least the following:

 (1) whether the design of the online service, product, or feature could lead to children experiencing or being targeted by contacts on the online service, product, or feature that would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (2) whether the design of the online service, product, or feature could permit children to witness, participate in, or be subject to conduct on the online service, product, or feature that would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (3) whether the design of the online service, product, or feature are reasonably expected to allow children to be party to or exploited by a contract on the online service, product, or feature that would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (4) whether algorithms used by the product, service, or feature could harm children or would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (5) whether targeted advertising systems used by the online service, product, or feature would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (6) whether the online service, product, or feature uses system design features to increase, sustain, or extend use of the online service, product, or feature by children, including the automatic playing of media, rewards for time spent, and notifications, that would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation;

 (7) whether, how, and for what purpose the online product, service, or feature collects or processes personal data of children, and whether those practices would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and severe psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation; and

 (8) whether and how product experimentation results for the online product, service, or feature reveal data management or design practices that would result in: reasonably foreseeable and material physical or financial harm to the child; reasonably foreseeable and extreme psychological or emotional harm to the child; a highly offensive intrusion on the reasonable privacy expectations of the child; or discrimination against the child based upon race, color, religion, national origin, disability, sex, or sexual orientation.

 (C) A data protection impact assessment conducted by a covered entity for the purpose of compliance with any other law complies with this section if the data protection impact assessment meets the requirements of this chapter.

 (D) A single data protection impact assessment may contain multiple similar processing operations that present similar risks only if each relevant online service, product, or feature is addressed.

 (E) A company may process only the personal data reasonably necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged to estimate age.

 Section 39‑79‑50. A covered entity that provides an online service, product, or feature reasonably likely to be accessed by children may not:

 (1) process the personal data of any child in a way that is inconsistent with the best interests of children reasonably likely to access the online service, product, or feature;

 (2) profile a child by default unless both of the following criteria are met:

 (a) the covered entity can demonstrate it has appropriate safeguards in place to ensure that profiling is consistent with the best interests of children reasonably likely to access the online service, product, or feature; and

 (b) either of the following is true:

 (i) profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which a child is actively and knowingly engaged;

or

 (ii) the covered entity can demonstrate a compelling reason that profiling is in the best interests of children;

 (3) process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged;

 (4) if the end user is a child, process personal data for any reason other than a reason for which that personal data was collected;

 (5) process any precise geolocation information of children by default, unless the collection of that precise geolocation information is strictly necessary for the covered entity to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature;

 (6) process any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected;

 (7) use dark patterns to cause children to provide personal data beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the covered entity knows, or has reason to know, is not in the best interests of children reasonably likely to access the online service, product, or feature; or

 (8) allow a child’s parent, guardian, or any other consumer to monitor the child’s online activity or track the child’s location, without providing an obvious signal to the child when the child is being monitored or tracked.

 Section 39‑79‑60. (A) A data protection impact assessment collected or maintained by the Attorney General pursuant to Section 39‑79‑40 is exempt from public disclosure pursuant to Section 30‑4‑10.

 (B) To the extent any information contained in a data protection impact assessment disclosed to the Attorney General includes information subject to attorney‑client privilege or work product protection, disclosure pursuant to this section does not constitute a waiver of such privilege or protection.

 Section 39‑79‑70. (A) A covered entity that violates this chapter may be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars for each affected child for each negligent violation or not more than seven thousand five hundred for each affected child for each intentional violation, which may be assessed or recovered only in a civil action brought by the Attorney General. If the State prevails in an action to enforce this chapter, the state may, in addition to penalties provided by this section or other remedies provided by the law, be allowed an amount determined by the court to be the reasonable value of all or part of the state’s litigation expenses incurred.

 (B) Any penalties, fees, and expenses recovered in an action brought pursuant to this chapter must be appropriated to the Attorney General to offset costs incurred by the Attorney General in connection with enforcement of this chapter.

 (C) If a covered entity is in substantial compliance with the requirements of Section 39‑79‑40, the Attorney General, before initiating a civil action under this section, shall provide written notice to the covered entity identifying the specific provisions of this chapter that the Attorney General alleges have been or are being violated. If, for a covered entity that satisfied the provisions of Section 39‑79‑40(A) before offering any new online product, service, or feature reasonably likely to be accessed by children to the public, within ninety days of the notice required by this section, the covered entity cures any noticed violation and provides the Attorney General a written statement that the alleged violations have been cured, and sufficient measures have been taken to prevent future violations, the covered entity is not liable for a civil penalty for any violation cured pursuant to this section.

 (D) Nothing in this chapter may be construed to create a private right of action pursuant to this chapter or to enforce the provisions of this chapter.

 Section 39‑79‑80. Nothing in this chapter may be interpreted or construed to:

 (1) impose liability in a manner that is inconsistent with 47 U.S.C. Section 230;

 (2) prevent or preclude any child from deliberately or independently searching for, or specifically requesting, content; or

 (3) require a covered entity to implement an age‑gating requirement.

SECTION 3. If any section, subsection, paragraph, subparagraph, sentence, clause, phrase, or word of this act is for any reason held to be unconstitutional or invalid, such holding shall not affect the constitutionality or validity of the remaining portions of this act, the General Assembly hereby declaring that it would have passed this act, and each and every section, subsection, paragraph, subparagraph, sentence, clause, phrase, and word thereof, irrespective of the fact that any one or more other sections, subsections, paragraphs, subparagraphs, sentences, clauses, phrases, or words hereof may be declared to be unconstitutional, invalid, or otherwise ineffective.

SECTION 4. (A) This act takes effect upon approval by the Governor.

 (B) By January first of the year following the effective date of this act, a covered entity must complete a data protection impact assessment for any online service, product, or feature reasonably likely to be accessed by children offered to the public before the effective date, unless that online service, product, or feature is exempt under subsection (C).

 (C) This act does not apply to an online service, product, or feature that is not offered to the public on or after January first of the year following the effective date.

‑‑‑‑XX‑‑‑‑