

GENERAL ASSEMBLY OF NORTH CAROLINA  
SESSION 2023

FILED SENATE  
Apr 3, 2023  
S.B. 525  
PRINCIPAL CLERK

S

D

SENATE BILL DRS35199-LR-18B

Short Title: Consumer Privacy Act.

(Public)

Sponsors: Senators Salvador, Moffitt, and Hanig (Primary Sponsors).

Referred to:

1 A BILL TO BE ENTITLED  
2 AN ACT TO PROTECT CONSUMERS BY ENACTING THE CONSUMER PRIVACY ACT  
3 OF NORTH CAROLINA.

4 The General Assembly of North Carolina enacts:

5 SECTION 1. This act shall be known and may be cited as the "North Carolina  
6 Consumer Privacy Act."

7 SECTION 2. The General Statutes are amended by adding a new Chapter to read:  
8 "Chapter 75F.  
9 "Consumer Privacy Act.

10 "§ 75F-1. Definitions.

11 (a) This Chapter shall be known and may be cited as the "North Carolina Consumer  
12 Privacy Act."

13 (b) Definitions. – The following definitions apply in this Chapter:

14 (1) Account. – The Consumer Privacy Restricted Account established in  
15 G.S. 75F-14.

16 (2) Affiliate. – An entity that (i) controls, is controlled by, or is under common  
17 control with another entity or (ii) shares common branding with another entity.

18 (3) Aggregated data. – Information that relates to a group or category of  
19 consumers (i) from which individual consumer identities have been removed  
20 and (ii) that is not linked or reasonably linkable to any consumer.

21 (4) Air carrier. – As defined in 49 U.S.C. § 40102.

22 (5) Authenticate. – To use reasonable means to determine that a consumer's  
23 request to exercise the rights described in G.S. 75F-4 is made by the consumer  
24 who is entitled to exercise those rights.

25 (6) Biometric data. – Data generated by automatic measurements of an  
26 individual's unique biological characteristics. The term includes an  
27 individual's fingerprint, voiceprint, eye retinas, irises, or any other unique  
28 biological pattern or characteristic that is used to identify a specific individual.  
29 Biometric data does not include any of the following:

30 a. A physical or digital photograph.

31 b. A video or audio recording.

32 c. Data generated from an item described in sub-subdivision a. or b. of  
33 this subdivision.

34 d. Information captured from a patient in a health care setting.



\* D R S 3 5 1 9 9 - L R - 1 8 B \*

- 1 e. Information collected, used, or stored for treatment, payment, or health  
2 care operations as those terms are defined in 45 C.F.R. Parts 160, 162,  
3 and 164.
- 4 (7) Business associate. – As defined in 45 C.F.R. § 160.103.  
5 (8) Child. – An individual younger than 13 years old.  
6 (9) Consent. – An affirmative act by a consumer that unambiguously indicates the  
7 consumer's voluntary and informed agreement to allow a person to process  
8 personal data related to the consumer.
- 9 (10) Consumer. – An individual who is a resident of this State acting in an  
10 individual or household context. The term does not include an individual  
11 acting in a commercial or employment context.
- 12 (11) Control or controlled. – Includes each of the following: (i) ownership of, or  
13 the power to vote, more than fifty percent (50%) of the outstanding shares of  
14 any class of voting securities of an entity; (ii) control in any manner over the  
15 election of a majority of the directors or of the individuals exercising similar  
16 functions; and (iii) the power to exercise controlling influence of the  
17 management of an entity.
- 18 (12) Controller. – A person doing business in this State who determines the  
19 purposes for which, and the means by which, personal data are processed,  
20 regardless of whether the person makes the determination alone or with others  
21 that, alone or jointly with others, determines the purpose and means of  
22 processing personal data.
- 23 (13) Covered entity. – As defined in 45 C.F.R. § 160.103.  
24 (14) De-identified data. – Data that cannot reasonably be linked to an identified or  
25 identifiable individual that are possessed by a controller who does all of the  
26 following:
- 27 a. Takes reasonable measures to ensure that a person cannot associate the  
28 data with an individual.
- 29 b. Publicly commits to maintain and use the data only in de-identified  
30 form and not attempt to reidentify the data.
- 31 c. Contractually obligates any recipients of the data to comply with the  
32 requirements described in sub-subdivisions a. and b. of this  
33 subdivision.
- 34 (15) Director. – The Director of the Division.  
35 (16) Division. – Consumer Protection Division of the North Carolina Department  
36 of Justice or other unit of the Department of Justice engaging in activities  
37 under this Chapter.
- 38 (17) Government entity. – The State or any local political subdivision of the State.  
39 (18) Health care facility. – Any entity licensed pursuant to Chapter 122C, 131D,  
40 or 131E of the General Statutes or Article 64 of Chapter 58 of the General  
41 Statutes, and any clinical laboratory certified under the federal Clinical  
42 Laboratory Improvement Amendments in section 353 of the Public Health  
43 Service Act (42 U.S.C. § 263a).
- 44 (19) Health care provider. – Includes:
- 45 a. An individual who is licensed, certified, or otherwise authorized under  
46 Chapter 90 or 90B of the General Statutes to provide health care  
47 services in the ordinary course of business or practice of a profession  
48 or in an approved education or training program.
- 49 b. A health care facility where health care services are provided to  
50 patients, residents, or others to whom such services are provided as  
51 allowed by law.

- 1           c.     Individuals licensed under Chapter 90 of the General Statutes or  
2           practicing under a waiver in accordance with G.S. 90-12.5.
- 3           d.     Any emergency medical services personnel as defined in  
4           G.S. 131E-155(7).
- 5           e.     Any individual who is employed as a health care facility administrator,  
6           executive, supervisor, board member, trustee, or other person in a  
7           managerial position or comparable role at a health care facility.
- 8           f.     An agent or employee of a health care facility that is licensed, certified,  
9           or otherwise authorized to provide health care services.
- 10          g.     An officer or director of a health care facility.
- 11          h.     An agent or employee of a health care provider who is licensed,  
12          certified, or otherwise authorized to provide health care services.
- 13          (20) Identifiable individual. – An individual who can be readily identified, directly  
14          or indirectly.
- 15          (21) Institution of higher education. – A public or private institution of higher  
16          education.
- 17          (22) Local political subdivision. – Includes a city, a county, a local school  
18          administrative unit as defined in G.S. 115C-5, or a community college.
- 19          (23) Nonprofit organization. – Any corporation exempt from taxation under  
20          section 501(c)(3), 501(c)(6), or 501(c)(12) of the Internal Revenue Code.
- 21          (24) Personal data. – Information that can be used to distinguish or trace an  
22          individual's identity, either alone or when combined with other information.  
23          The term does not include information that is a public record under Chapter  
24          132 of the General Statutes or information made available to the general  
25          public lawfully and intentionally.
- 26          (25) Process. – Any operation or set of operations performed on personal data,  
27          including collection, use, storage, disclosure, analysis, deletion, or  
28          modification of personal data.
- 29          (26) Processor. – A person who processes personal data on behalf of a controller.
- 30          (27) Protected health information. – As defined in 45 C.F.R. § 160.103.
- 31          (28) Pseudonymous data. – Personal data that cannot be attributed to a specific  
32          individual without the use of additional information, if the additional  
33          information is (i) kept separately from the consumer's personal data and (ii)  
34          subject to appropriate technical and organizational measures to ensure that the  
35          personal data is not attributable to an identified or identifiable individual.
- 36          (29) Publicly available information. – Information that a person (i) lawfully obtains  
37          from a record of a governmental entity, (ii) reasonably believes a consumer or  
38          widely distributed media has lawfully made available to the general public, or  
39          (iii) if the consumer has not restricted the information to a specific audience,  
40          obtains from a person to whom the consumer disclosed the information.
- 41          (30) Right. – A consumer right described in G.S. 75F-4.
- 42          (31) Sale, sell, or sold. – The exchange of personal data for monetary consideration  
43          by the controller to a third party. The terms do not include any of the  
44          following:
- 45               a.     A controller's disclosure of personal data to a processor who processes  
46               the personal data on behalf of the controller.
- 47               b.     A controller's disclosure of personal data to an affiliate of the  
48               controller.
- 49               c.     Considering the context in which the consumer provided the personal  
50               data to the controller, a controller's disclosure of personal data to a

- 1 third party if the purpose is consistent with a consumer's reasonable  
2 expectations.
- 3 d. The disclosure or transfer of personal data when a consumer directs a  
4 controller to disclose the personal data or interact with one or more  
5 third parties.
- 6 e. A consumer's disclosure of personal data to a third party for the  
7 purpose of providing a product or service requested by the consumer  
8 or a parent or legal guardian of a child.
- 9 f. The disclosure of information that the consumer intentionally makes  
10 available to the general public via a channel of mass media and does  
11 not restrict to a specific audience.
- 12 g. A controller's transfer of personal data to a third party as an asset that  
13 is part of a proposed or actual merger, acquisition, or bankruptcy in  
14 which the third party assumes control of all or part of the controller's  
15 assets.
- 16 (32) Sensitive data. – Personal data that reveals any of the following:
- 17 a. An individual's (i) racial or ethnic origin, (ii) religious beliefs, (iii)  
18 sexual orientation, (iv) citizenship or immigration status, or (v)  
19 information regarding an individual's medical history, mental or  
20 physical health condition, or medical treatment or diagnosis by a  
21 health care professional. The term does not include personal data that  
22 reveals an individual's racial or ethnic origin if the personal data are  
23 processed by a video communication service. If the personal data are  
24 processed by a person licensed to provide health care under State or  
25 federal law, information regarding an individual's medical history,  
26 mental or physical health condition, or medical treatment or diagnosis  
27 by a health care professional, then the personal data is not sensitive  
28 data.
- 29 b. The processing of genetic or biometric data if the processing is for the  
30 purpose of identifying a specific individual.
- 31 c. Specific geolocation data.
- 32 (33) Specific geological location. – Information derived from technology,  
33 including global positioning system level latitude and longitude coordinates,  
34 that directly identifies an individual's specific location, accurate within a  
35 radius of 1,750 feet or less. The term does not include (i) the content of a  
36 communication or (ii) any data generated by or connected to advanced utility  
37 metering infrastructure systems or equipment used by a utility.
- 38 (34) Targeted advertising. – Displaying an advertisement to a consumer where the  
39 consumer is selected based upon personal data obtained from the consumer's  
40 activities over time and across nonaffiliated websites or online applications to  
41 predict the consumer's preferences and interests. The term does not include  
42 any advertising:
- 43 a. Based upon a consumer's activities within the controller's website or  
44 online application or any affiliated website or online application.
- 45 b. Based on the context of a consumer's current search query or visit to a  
46 website or online application.
- 47 c. Directed to a consumer in response to the consumer's request for  
48 information, product, a service, or feedback.
- 49 d. Processing personal data solely to measure or report advertising  
50 performance, reach, or frequency.

- 1           (35) Third party. – A person other than the consumer, controller, or processor or  
2 an affiliate or contractor of the controller or processor.
- 3           (36) Trade secret. – Information, including a formula, pattern, compilation,  
4 program, device, method, technique, or process that (i) derives independent  
5 economic value, actual or potential, from not being generally known to and  
6 not being readily ascertainable by proper means by other persons who can  
7 obtain economic value from the information's disclosure or use and (ii) is the  
8 subject of efforts that are reasonable under the circumstances to maintain the  
9 information's secrecy.

10 **§ 75F-2. Applicability.**

- 11       (a) This Chapter applies to any controller or processor who:
- 12           (1) Conducts business in this State or produces a product or service that is targeted  
13 to consumers who are residents of this State;
- 14           (2) Has annual revenue of twenty-five million dollars (\$25,000,000) or more; and
- 15           (3) Satisfies one or more of the following thresholds:
- 16               a. During a calendar year, controls or processes personal data of 100,000  
17 or more consumers; or
- 18               b. Derives over fifty percent (50%) of the entity's gross revenue from the  
19 sale of personal data and controls or processes personal data of 25,000  
20 or more consumers.
- 21       (b) This Chapter does not apply to any of the following:
- 22           (1) A governmental entity or a third party under contract with a governmental  
23 entity when the third party is acting on behalf of the governmental entity.
- 24           (2) A tribe.
- 25           (3) An institution of higher education.
- 26           (4) A nonprofit corporation.
- 27           (5) A covered entity.
- 28           (6) A business associate.
- 29           (7) Information that meets the definition of one of the following:
- 30               a. Protected health information for purposes of the federal Health  
31 Insurance Portability and Accountability Act of 1996, 42 U.S.C. §  
32 1320d et seq., and related regulations.
- 33               b. Patient identifying information for purposes of 42 C.F.R. Part 2.
- 34               c. Identifiable private information for purposes of the federal Policy for  
35 the Protection of Human Subjects, 45 C.F.R. Part 46.
- 36               d. Identifiable private information or personal data collected as part of  
37 human subjects research pursuant to or under the same standards as:
- 38                   1. The good clinical practice guidelines issued by the  
39 International Council for Harmonisation; or
- 40                   2. The Protection of Human Subjects under 21 C.F.R. Part 50 and  
41 Institutional Review Boards under 21 C.F.R. Part 56.
- 42               e. Personal data used or shared in research conducted in accordance with  
43 one or more of the requirements described in sub-subdivision b. of this  
44 subdivision.
- 45               f. Information and documents created for purposes of the federal Health  
46 Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq., and  
47 related regulations.
- 48               g. Patient safety work product for purposes of 42 C.F.R. Part 3; or
- 49               h. Information that is:
- 50                   1. De-identified in accordance with the requirements for  
51 de-identification set forth in 45 C.F.R. Part 164; and

- 1                                    2. Derived from any of the health care-related information listed  
2                                    above in this subdivision.
- 3           (8)   Information originating from, and intermingled to be indistinguishable with,  
4                                    information under subdivision (7) of this subsection that is maintained by a (i)  
5                                    health care facility or health care provider or (ii) program or a qualified service  
6                                    organization as defined in 42 C.F.R. § 2.11.
- 7           (9)   Information used only for public health activities and purposes as described  
8                                    in 45 C.F.R. § 164.512.
- 9           (10)   An activity:
- 10                                  a.   Subject to regulation under the federal Fair Credit Reporting Act, 15  
11                                  U.S.C. § 1681 et seq., by one of the following:
- 12    1.   A consumer reporting agency, as defined in 15 U.S.C. § 1681a;  
13    2.   A furnisher of information, as set forth in 15 U.S.C. § 1681s-2,  
14    who provides information for use in a consumer report, as  
15    defined in 15 U.S.C. § 1681a; or  
16    3.   A user of a consumer report, as set forth in 15 U.S.C. § 1681b;  
17    and
- 18                                  b.   Involving the collection, maintenance, disclosure, sale,  
19                                  communication, or use of any personal data bearing on a consumer's  
20                                  credit worthiness, credit standing, credit capacity, character, general  
21                                  reputation, personal characteristics, or mode of living.
- 22           (11)   A financial institution or an affiliate of a financial institution governed by, or  
23                                  personal data collected, processed, sold, or disclosed in accordance with, Title  
24                                  V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and related  
25                                  regulations.
- 26           (12)   Personal data collected, processed, sold, or disclosed in accordance with the  
27                                  federal Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.
- 28           (13)   Personal data regulated by the federal Family Education Rights and Privacy  
29                                  Act, 20 U.S.C. § 1232g, and related regulations.
- 30           (14)   Personal data collected, processed, sold, or disclosed in accordance with the  
31                                  federal Farm Credit Act of 1971, 12 U.S.C. § 2001 et seq.
- 32           (15)   Data that are processed or maintained:
- 33                                  a.   In the course of an individual applying to, being employed by, or  
34                                  acting as an agent or independent contractor of a controller, processor,  
35                                  or third party to the extent the collection and use of the data are related  
36                                  to the individual's role;
- 37                                  b.   As the emergency contact information of an individual described in  
38                                  sub-subdivision a. of this subdivision and used for emergency contact  
39                                  purposes; or
- 40                                  c.   To administer benefits for another individual relating to an individual  
41                                  described in sub-subdivision a. of this subdivision and used for the  
42                                  purpose of administering the benefits.
- 43           (16)   An individual's processing of personal data for purely personal or household  
44                                  purposes.
- 45           (17)   An air carrier.
- 46           (c)   A controller is in compliance with any obligation to obtain parental consent under this  
47                                  Chapter if the controller complies with the verifiable parental consent mechanisms under the  
48                                  Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq., and the act's implementing  
49                                  regulations and exemptions.

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

4 **"§ 75F-3. Preemption; reference to other laws.**

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

8       (b) Any reference to federal law in this Chapter includes any rules or regulations  
9 promulgated under the federal law.

10 **"§ 75F-4. Consumer rights; access; deletion; portability; opt out of certain processing.**

11       (a) A consumer has the right to:

12           (1) Confirm whether a controller is processing the consumer's personal data and  
13 access the consumer's personal data.

14           (2) Delete the consumer's personal data that the consumer provided to the  
15 controller.

16           (3) Obtain a copy of the consumer's personal data that the consumer previously  
17 provided to the controller, in a format that to the extent technically feasible,  
18 that is readily usable and allows the consumer to transmit the data to another  
19 controller without impediment where the processing is carried out by  
20 automated means.

21           (4) Opt out of the processing of the consumer's personal data for purposes of  
22 targeted advertising or the sale of personal data.

23       (b) Nothing in this section requires a person to cause a breach of security system.

24 **"§ 75F-5. Exercising consumer rights.**

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

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

29       (c) In the case of processing personal data concerning a consumer subject to  
30 guardianship, the guardian of the consumer shall exercise a right on the consumer's behalf.

31 **"§ 75F-6. Controller's response to requests.**

32       (a) Subject to the other provisions of this Chapter, a controller shall comply with a  
33 consumer's request under G.S. 75F-5 to exercise a right.

34       (b) Within 45 days after the day on which a controller receives a request to exercise a  
35 right, the controller shall take action on the consumer's request and inform the consumer of any  
36 action taken on the consumer's request.

37       (c) The controller may extend once the initial 45-day period by an additional 45 days if  
38 reasonably necessary due to the complexity of the request or the volume of the requests received  
39 by the controller. If a controller extends the initial 45-day period, before the initial 45-day period  
40 expires, the controller shall (i) inform the consumer of the extension, including the length of the  
41 extension, and (ii) provide the reasons the extension is reasonably necessary.

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

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

48       (f) A controller may not charge a fee for information in response to a request, unless the  
49 request is the consumer's second or subsequent request during the same 12-month period.  
50 However, a controller may charge a reasonable fee to cover the administrative costs of complying  
51 with a request or refuse to act on a request if:

- 1           (1) The request is excessive, repetitive, technically infeasible, or manifestly  
2           unfounded;  
3           (2) The controller reasonably believes the primary purpose in submitting the  
4           request was something other than exercising a right; or  
5           (3) The request, individually or as part of an organized effort, harasses, disrupts,  
6           or imposes undue burden on the resources of the controller's business.

7           (g) A controller that charges a fee or refuses to act in accordance with this section bears  
8 the burden of demonstrating the request satisfied one or more of the criteria described in this  
9 section.

10          (h) If a controller is unable to authenticate a consumer request to exercise a right  
11 described in G.S. 75F-4 using commercially reasonable efforts, the controller is not required to  
12 comply with the request and may request that the consumer provide additional information  
13 reasonably necessary to authenticate the request.

14 **"§ 75F-7. Responsibilities according to role.**

15          (a) A processor shall adhere to the controller's instructions, and taking into account the  
16 nature of the processing and information available to the processor, by appropriate technical and  
17 organizational measures, insofar as reasonably practicable, assist the controller in meeting the  
18 controller's obligations, including obligations related to the security of processing personal data  
19 and notification of a breach of security system.

20          (b) Before a processor performs processing on behalf of a controller, the processor and  
21 controller shall enter into a contract that does all of the following:

- 22           (1) Clearly sets forth instructions for processing personal data, the nature and  
23 purpose of the processing, the type of data subject to processing, the duration  
24 of the processing, and the parties' rights and obligations.  
25           (2) Requires the processor to ensure each person processing personal data is  
26 subject to a duty of confidentiality with respect to the personal data.  
27           (3) Requires the processor to engage any subcontractor pursuant to a written  
28 contract that requires the subcontractor to meet the same obligations as the  
29 processor with respect to the personal data.

30          (c) Determining whether a person is acting as a controller or processor with respect to a  
31 specific processing of data is a fact-based determination that depends upon the context in which  
32 personal data are to be processed. A processor that adheres to a controller's instructions with  
33 respect to a specific processing of personal data remains a processor.

34 **"§ 75F-8. Responsibilities of contractors; transparency; purpose specification and data**  
35 **minimization; consent for secondary use; security; nondiscrimination.**

36          (a) A controller shall provide consumers with a reasonably accessible and clear privacy  
37 notice that includes all of the following:

- 38           (1) The categories of personal data processed by the controller.  
39           (2) The purposes for which the categories of personal data are processed.  
40           (3) How consumers may exercise a right.  
41           (4) The categories of personal data that the controller shares with third parties, if  
42 any.  
43           (5) The categories of third parties, if any, with whom the controller shares  
44 personal data.

45 If a controller sells a consumer's personal data to one or more third parties or engages in targeted  
46 advertising, the controller shall clearly and conspicuously disclose to the consumer the manner  
47 in which the consumer may exercise the right to opt out of the sale of the consumer's personal  
48 data or processing for targeted advertising.

49          (b) A controller shall establish, implement, and maintain reasonable administrative,  
50 technical, and physical data security practices designed to protect the confidentiality and integrity  
51 of personal data and reduce reasonably foreseeable risks of harm to consumers relating to the



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

4 (c) Except as otherwise provided in this Chapter, a controller may not process sensitive  
5 data collected from a consumer without first presenting the consumer with clear notice and an  
6 opportunity to opt out of the processing, or in the case of the processing of personal data  
7 concerning a known child, processing the data in accordance with the federal Children's Online  
8 Privacy Protection Act, 15 U.S.C. § 6501 et seq., and the act's implementing regulations and  
9 exemptions.

10 (d) A controller may not discriminate against a consumer for exercising a right by (i)  
11 denying a good or service to the consumer, (ii) charging the consumer a different price or rate  
12 for a good or service, or (iii) providing the consumer a different level of quality of a good or  
13 service. Nothing in this subsection prohibits a controller from offering a different price, rate,  
14 level, quality, or selection of a good or service to a consumer, including offering a good or service  
15 for no fee or at a discount, if the consumer has opted out of targeted advertising or the offer is  
16 related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium  
17 features, discounts, or club card program.

18 (e) A controller is not required to provide a product, service, or functionality to a  
19 consumer if the consumer's personal data are, or the processing of the consumer's personal data  
20 is, reasonably necessary for the controller to provide the consumer the product, service, or  
21 functionality and the consumer does not provide the consumer's personal data to the controller  
22 or allow the controller to process the consumer's personal data. Any provision of a contract that  
23 purports to waive or limit a consumer's right under this Chapter is void.

24 **"§ 75F-9. Processing de-identified data or pseudonymous data.**

25 (a) The provisions of this Chapter do not require a controller or processor to do any of  
26 the following:

27 (1) Reidentify de-identified data or pseudonymous data.

28 (2) Maintain data in identifiable form or obtain, retain, or access any data or  
29 technology for the purpose of allowing the controller or processor to associate  
30 a consumer request with personal data.

31 (3) Comply with an authenticated consumer request to exercise a right described  
32 in G.S. 75F-4, if the controller:

33 a. Is not reasonably capable of associating the request with the personal  
34 data or it would be unreasonably burdensome for the controller to  
35 associate the request with the personal data;

36 b. Does not (i) use the personal data to recognize or respond to the  
37 consumer who is the subject of the personal data or (ii) associate the  
38 personal data with other personal data about the consumer; and

39 c. Does not sell or otherwise disclose the personal data to any third  
40 party other than a processor, except as otherwise permitted in this  
41 section.

42 (b) The rights described in G.S. 75F-4(a)(1) through (a)(3) do not apply to pseudonymous  
43 data if a controller demonstrates that any information necessary to identify a consumer is kept  
44 separately and subject to appropriate technical and organizational measures to ensure the  
45 personal data are not attributed to an identified individual or an identifiable individual.

46 (c) A controller who uses pseudonymous data or de-identified data shall take reasonable  
47 steps to ensure the controller complies with any contractual obligations to which the  
48 pseudonymous data or de-identified data are subject and promptly addresses any breach of a  
49 contractual obligation.

50 **"§ 75F-10. Limitations.**

- 1       (a)    The requirements described in this Chapter do not restrict a controller's or processor's  
2 ability to do any of the following:
- 3           (1)    Comply with a State, federal, or local law, rule, or regulation.  
4           (2)    Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena,  
5 or summons by a federal, State, local, or other governmental entity.  
6           (3)    Cooperate with a law enforcement agency concerning activity that the  
7 controller or processor reasonably and in good faith believes may violate  
8 federal, State, or local laws, rules, or regulations.  
9           (4)    Investigate, establish, exercise, prepare for, or defend a legal claim.  
10          (5)    Provide a product or service requested by a consumer or a parent or legal  
11 guardian of a child.  
12          (6)    Perform a contract to which the consumer or the parent or legal guardian of a  
13 child is a party, including fulfilling the terms of a written warranty or taking  
14 steps at the request of the consumer or parent or legal guardian before entering  
15 into the contract with the consumer.  
16          (7)    Take immediate steps to protect an interest that is essential for the life or  
17 physical safety of the consumer or of another individual.  
18          (8)    Detect, prevent, protect against, or respond to a security incident, identity  
19 theft, fraud, harassment, malicious or deceptive activity, or any illegal activity  
20 or investigate, report, or prosecute a person responsible for an action described  
21 in this subdivision.  
22          (9)    Preserve the integrity or security of systems or investigate, report, or prosecute  
23 a person responsible for harming or threatening the integrity or security of  
24 systems.  
25          (10)   If the controller discloses the processing in a notice described in G.S. 75F-8,  
26 engage in public or peer-reviewed scientific, historical, or statistical research  
27 in the public interest that adheres to all other applicable ethics and privacy  
28 laws.  
29          (11)   Assist another person with an obligation described in this subsection.  
30          (12)   Process personal data to do any of the following:  
31           a.     Conduct internal analytics or other research to develop, improve, or  
32 repair a controller's or processor's product, service, or technology.  
33           b.     Identify and repair technical errors that impair existing or intended  
34 functionality.  
35           c.     Effectuate a product recall.  
36          (13)   Process personal data to perform an internal operation that is (i) reasonably  
37 aligned with the consumer's expectations based on the consumer's existing  
38 relationship with the controller or (ii) otherwise compatible with processing  
39 to aid the controller or processor in providing a product or service specifically  
40 requested by a consumer or a parent or legal guardian of a child or the  
41 performance of a contract to which the consumer or a parent or legal guardian  
42 of a child is a party.  
43          (14)   Retain a consumer's email address to comply with the consumer's request to  
44 exercise a right.
- 45       (b)    This Chapter does not apply if a controller's or processor's compliance with this  
46 Chapter:
- 47           (1)    Violates an evidentiary privilege under North Carolina law.  
48           (2)    As part of a privileged communication, prevents a controller or processor from  
49 providing personal data concerning a consumer to a person covered by an  
50 evidentiary privilege under North Carolina law.  
51           (3)    Adversely affects the privacy or other rights of any person.

1 (c) A controller or processor is not in violation of this Chapter if:

2 (1) The controller or processor discloses personal data to a third-party controller  
3 or processor in compliance with this Chapter.

4 (2) The third party processes the personal data in violation of this Chapter.

5 (3) The disclosing controller or processor did not have actual knowledge of the  
6 third party's intent to commit a violation of this Chapter.

7 (d) If a controller processes personal data under an exemption described in subsection (a)  
8 of this section, the controller bears the burden of demonstrating that the processing qualifies for  
9 the exemption.

10 (e) Nothing in this Chapter requires a controller, processor, third party, or consumer to  
11 disclose a trade secret.

12 **"§ 75F-11. No private cause of action.**

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

15 **"§ 75F-12. Enforcement.**

16 (a) The Division shall establish and administer a system to receive consumer complaints  
17 regarding a controller's or processor's alleged violation of this Chapter.

18 (b) The Division may investigate a consumer complaint to determine whether the  
19 controller or processor violated or is violating this Chapter.

20 **"§ 75F-13. Enforcement powers of the Attorney General.**

21 (a) The Attorney General has the exclusive authority to enforce this Chapter. Upon  
22 referral from the Division, the Attorney General may initiate an enforcement action against a  
23 controller or processor for a violation of this Chapter.

24 (b) At least 45 days before the day on which the Attorney General initiates an  
25 enforcement action against a controller or processor, the Attorney General shall provide the  
26 controller or processor with the following:

27 (1) Written notice identifying each provision of this Chapter the Attorney General  
28 alleges the controller or processor has violated or is violating.

29 (2) An explanation of the basis for each allegation.

30 (c) The Attorney General may not initiate an action if the controller or processor:

31 (1) Cures the noticed violation within 45 days after the day on which the  
32 controller or processor receives the written notice described in subsection (b)  
33 of this section.

34 (2) Provides the Attorney General an express written statement that the violation  
35 has been cured and no further violation of the cured violation will occur.

36 (d) The Attorney General may initiate an action against a controller or processor who (i)  
37 fails to cure a violation after receiving the notice described in subsection (b) of this section or (ii)  
38 after curing a noticed violation and providing a written statement in accordance with subsection  
39 (b) of this section, continues to violate this Chapter.

40 (e) In an action described in subsection (d) of this section, the Attorney General may  
41 recover actual damages to the consumer; and for each violation described in subsection (d) of  
42 this section, an amount not to exceed seven thousand five hundred dollars (\$7,500).

43 (f) All money received from an action under this Chapter shall be deposited into the  
44 Consumer Privacy Account established in G.S. 75F-14.

45 (g) If more than one controller or processor are involved in the same processing in  
46 violation of this Chapter, the liability for the violation shall be allocated among the controllers or  
47 processors in proportion to the comparative fault of each controller or processor.

48 **"§ 75F-14. Consumer Privacy Account.**

49 (a) There is created a restricted account known as the "Consumer Privacy Account." The  
50 account shall be funded by money received through civil enforcement actions under this Chapter.

1       (b) Upon appropriation by the General Assembly, the account funds may be used by the  
2 Attorney General for these purposes:

3           (1) Investigation and administrative costs incurred by the Division in  
4 investigating consumer complaints alleging violations of this Chapter.

5           (2) Recovery of costs and attorney fees accrued by the Attorney General in  
6 enforcing this Chapter.

7           (3) Providing consumer and business education regarding consumer rights under  
8 this Chapter and compliance with the provisions of this Chapter for controllers  
9 and processors.

10       (c) If the balance in the account exceeds four million dollars (\$4,000,000) at the close of  
11 any fiscal year, the State Budget Director shall transfer the amount that exceeds four million  
12 dollars (\$4,000,000) into the General Fund.

13 **"§ 75F-15. Attorney General report.**

14       (a) The Attorney General and the Division shall compile a report evaluating the liability  
15 and enforcement provisions of this Chapter, including the effectiveness of the Attorney General's  
16 and the Division's efforts to enforce this Chapter and summarizing the data protected and not  
17 protected by this Chapter, including, with reasonable detail, a list of the types of information that  
18 are publicly available from State, local, and federal government sources.

19       (b) The Attorney General and the Division may update the report as new information  
20 becomes available.

21       (c) The Attorney General and the Division shall submit the report to the Joint Legislative  
22 Oversight Commission on Governmental Operations by July 1, 2025."

23       **SECTION 3.** This act becomes effective January 1, 2024.