

SENATE, No. 1389

STATE OF NEW JERSEY
221st LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2024 SESSION

Sponsored by:

Senator TROY SINGLETON

District 7 (Burlington)

Co-Sponsored by:

Senators Greenstein and Pou

SYNOPSIS

Requires notification to consumers of collection and disclosure of personal data by certain entities.

CURRENT VERSION OF TEXT

Introduced Pending Technical Review by Legislative Counsel.



1 AN ACT concerning online services, consumers, and personal data
2 and supplementing Title 56 of the Revised Statutes.

3

4 **BE IT ENACTED** by the Senate and General Assembly of the State
5 of New Jersey:

6

7 1. As used in P.L. , c. (C.) (pending before the
8 Legislature as this bill):

9 “Affiliate” means a legal entity that controls, is controlled by, or
10 is under common control with another legal entity. For the
11 purposes of this definition, “control” means: the ownership of or the
12 power to vote, more than 50 percent of the outstanding shares of
13 any class of voting security of a company; the control in any
14 manner over the election of a majority of the directors or
15 individuals exercising similar functions; or the power to exercise a
16 controlling influence over the management or policies of a
17 company.

18 “Biometric data” means data generated by automatic or
19 technological processing, measurements, or analysis of an
20 individual’s biological, physical, or behavioral characteristics,
21 including, but not limited to, fingerprint, voiceprint, eye retinas,
22 irises, facial mapping, facial geometry, facial templates, or other
23 unique biological, physical, or behavioral patterns or characteristics
24 that are used or intended to be used, singularly or in combination
25 with each other or with other personal data, to identify a specific
26 individual. “Biometric data” shall not include: a digital or physical
27 photograph; an audio or video recording; or any data generated
28 from a digital or physical photograph, or an audio or video
29 recording, unless such data is generated to identify a specific
30 individual.

31 “Child” shall have the same meaning as provided in COPPA.

32 “Consent” means a clear affirmative act signifying a consumer’s
33 freely given, specific, informed and unambiguous agreement to
34 allow the processing of personal data relating to the consumer.
35 “Consent” may include a written statement, including by electronic
36 means, or any other unambiguous affirmative action. “Consent shall
37 not include: acceptance of a general or broad terms of use or similar
38 document that contains descriptions of personal data processing
39 along with other, unrelated information; hovering over, muting,
40 pausing, or closing a given piece of content; or agreement obtained
41 through the use of dark patterns.

42 “Consumer” means an identified person who is a resident of this
43 State acting only in an individual or household context. “Consumer”
44 shall not include a person acting in a commercial or employment
45 context.

46 “Controller” means an individual, or legal entity that, alone or
47 jointly with others determines the purpose and means of processing
48 personal data.

1 “COPPA” means the federal Children’s Online Privacy
2 Protection Act, 15 U.S.C. s.6501 et seq., and any rules, regulations,
3 guidelines, and exceptions thereto, as may be amended from time to
4 time.

5 “Dark pattern” means a user interface designed or manipulated
6 with the substantial effect of subverting or impairing user
7 autonomy, decision-making, or choice, and includes, but is not
8 limited to, any practice the United States Federal Trade
9 Commission refers to as a “dark pattern.”

10 “Decisions that produce legal or similarly significant effects
11 concerning the consumer” means decisions that result in the
12 provision or denial of financial or lending services, housing,
13 insurance, education enrollment or opportunity, criminal justice,
14 employment opportunities, health care services, or access to
15 essential goods and services.

16 “De-identified data” means: data that cannot be reasonably used
17 to infer information about, or otherwise be linked to, an identified or
18 reasonably identifiable individual, or a device linked to such an
19 individual, if the controller that possesses the data: (1) takes
20 reasonable measures to ensure that the data cannot be associated with
21 an individual, (2) publicly commits to maintain and use the data only
22 in a de-identified fashion and not to attempt to re-identify the data,
23 and (3) contractually obligates any recipients of the information to
24 comply with the requirements of this paragraph.

25 “Designated request address” means an electronic mail address,
26 Internet website, or toll-free telephone number that a consumer may
27 use to request the information required to be provided pursuant to
28 section 3 of P.L. , c. (C.) (pending before the Legislature as
29 this bill).

30 “Personal data” means any information that is linked or
31 reasonably linkable to an identified or identifiable person. “Personal
32 data” shall not include de-identified data or publicly available
33 information.

34 “Precise geolocation data” means information derived from
35 technology, including, but not limited to, global positioning system
36 level latitude and longitude coordinates or other mechanisms, that
37 directly identifies the specific location of an individual with
38 precision and accuracy within a radius of 1,750 feet. “Precise
39 geolocation data” does not include the content of communications,
40 or any data generated by or connected to advanced utility metering
41 infrastructure systems or equipment for use by a utility.

42 “Process” or “processing” means an operation or set of
43 operations performed, whether by manual or automated means, on
44 personal data or on sets of personal data, such as the collection, use,
45 storage, disclosure, analysis, deletion, or modification of personal
46 data, and also includes the actions of a controller directing a
47 processor to process personal data.

1 “Processor” means a person, private entity, public entity, agency,
2 or other entity that processes personal data on behalf of the
3 controller.

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

9 “Publicly available information” means information that is
10 lawfully made available from federal, State, or local government
11 records, or widely-distributed media or information that a controller
12 has a reasonable basis to believe a consumer has lawfully made
13 available to the general public and has not restricted to a specific
14 audience.

15 “Sale” means the sharing, disclosing, or transferring of personal
16 data for monetary or other valuable consideration by the controller to a
17 third party. “Sale” shall not include:

18 The disclosure of personal data to a processor that only processes
19 the personal data on the controller’s behalf;

20 The disclosure of personal data to a third party for the purposes of
21 providing a product or service requested by the consumer;

22 The disclosure or transfer of personal data to an affiliate of the
23 controller;

24 The disclosure of personal data that the consumer intentionally
25 made available to the general public through a mass media channel
26 and did not restrict to a specific audience; or

27 The disclosure or transfer of personal data to a third party as an
28 asset that is part of a proposed or actual merger, acquisition,
29 bankruptcy, or other transaction in which the third party assumes
30 control of all or part of the controller’s assets.

31 “Sensitive data” means personal data revealing racial or ethnic
32 origin; religious beliefs; mental or physical health condition, treatment,
33 or diagnosis; financial information; sex life or sexual orientation;
34 citizenship or immigration status; status as transgender or non-binary;
35 genetic or biometric data that may be processed for the purpose of
36 uniquely identifying an individual; personal data collected from a
37 known child; or precise geolocation data.

38 “Targeted advertising” means displaying an advertisements to a
39 consumer where the advertisement is selected based on personal data
40 obtained or inferred from that consumer’s activities over time and
41 across nonaffiliated Internet web sites or online applications to predict
42 such consumer’s preferences or interests. “Targeted advertising” shall
43 not include: advertisements based on activities within a controller’s
44 own internet websites or online applications; advertisements based on
45 the context of a consumer’s current search query, visit to an internet
46 website or online application; advertisements directed to a consumer in
47 response to the consumer’s request for information or feedback; or

1 processing personal data solely to measure or report advertising
2 frequency, performance, or reach.

3 “Third party” means a person, private entity, public entity,
4 agency, or entity other than the consumer, controller, or affiliate or
5 processor of the controller.

6 “Trade secret” has the same meaning as section 2 of P.L.2011,
7 c.161 (C.56:15-2).

8 "Verified request" means the process through which a consumer
9 may submit a request to exercise a right or rights established in
10 P.L. , c. (C.) (pending before the Legislature as this bill),
11 and by which a controller can reasonably authenticate the request
12 and the consumer making the request using commercially
13 reasonable means.

14

15 2. Notwithstanding any State law, rule, regulation, or order to
16 the contrary, the provisions of P.L. , c. (C.) (pending
17 before the Legislature as this bill) shall only apply to controllers
18 that conduct business in the State or produce products or services
19 that are targeted to residents of the State, and that during a calendar
20 year either:

21 a. control or process the personal data of at least 100,000
22 consumers, excluding personal data processed solely for the
23 purpose of completing a payment transaction; or

24 b. control or process the personal data of at least 25,000
25 consumers and the controller derives revenue, or receives a discount
26 on the price of any goods or services, from the sale of personal data.

27

28 3. a. A controller shall provide to a consumer a reasonably
29 accessible, clear, and meaningful privacy notice that shall include, but
30 may not be limited to:

31 (1) the categories of the personal data that the controller
32 processes;

33 (2) the purpose for processing personal data;

34 (3) the categories of all third parties to which the controller may
35 disclose a consumer’s personal data;

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

38 (5) how consumers may exercise their consumer rights, including
39 the controller’s contact information and how a consumer may
40 appeal a controller’s decision with regard to the consumer’s
41 request;

42 (6) the process by which the controller notifies consumers of
43 material changes to the notification required to be made available
44 pursuant to this subsection, along with the effective date of the
45 notice; and

46 (7) an active electronic mail address or other online mechanism that
47 the consumer may use to contact the controller.

1 b. If a controller sells personal data to third parties or processes
2 personal data for the purposes of targeted advertising, the sale of
3 personal data, or profiling in furtherance of decisions that produce
4 legal or similarly significant effects concerning a consumer, the
5 controller shall clearly and conspicuously disclose such sale or
6 processing, as well as the manner in which a consumer may
7 exercise the right to opt out of such sale or processing, a description
8 of the process for a consumer to review and make requests pursuant
9 to section 4 of this act, P.L. , c. (C.) (pending before the
10 Legislature as this bill).

11 c. A controller shall not:

12 (1) require a consumer to create a new account in order to exercise
13 a right; or

14 (2) based solely on the exercise of a right and unrelated to
15 feasibility or the value of a service, increase the cost of, or decrease
16 the availability of, the product or service.

17
18 4. a. A controller that receives a verified request from a
19 consumer shall provide a response to the consumer within 45 days
20 of the controller's receipt of the request . The controller may extend
21 the response period by 45 additional days where reasonably
22 necessary, considering the complexity and number of the
23 consumer's requests, provided that the controller informs the
24 consumer of any such extension within the initial 45-day response
25 period and the reason for the extension and shall provide the
26 information for all disclosures of personal data that occurred in the
27 prior 12 months.

28 b. This section shall not apply to personal data collected prior to
29 the effective date of P.L. , c. (C.) (pending before the
30 Legislature as this bill) unless the controller continues to process
31 such information thereafter.

32 c. If a controller declines to take action regarding the consumer's
33 request, the controller shall inform the consumer without undue delay,
34 but not later than 45 days after receipt of the request, of the
35 justification for declining to take action and instructions for how to
36 appeal the decision.

37 d. Information provided in response to a consumer request shall be
38 provided by a controller, free of charge, once per consumer during any
39 twelve-month period, except that, for a second or subsequent identical
40 request within a 12-month period, the controller may charge an
41 amount calculated pursuant to regulations. If requests from a
42 consumer are manifestly unfounded, excessive, or repetitive, the
43 controller may charge the consumer a reasonable fee to cover the
44 administrative costs of complying with the request or decline to act on
45 the request. The controller shall bear the burden of demonstrating the
46 manifestly unfounded, excessive or repetitive nature of the request.

47 e. If a controller is unable to authenticate a request to exercise any
48 of the rights afforded under section 5 of P.L. , c. (C.)

1 (pending before the Legislature as this bill) using commercially
2 reasonable efforts, the controller shall not be required to comply with a
3 request to initiate an action pursuant to this section and shall provide
4 notice to the consumer that the controller is unable to authenticate the
5 request to exercise such right or rights until such consumer provides
6 additional information reasonably necessary to authenticate such
7 consumer and such consumer's request to exercise such right or rights.
8 A controller shall not be required to authenticate an opt-out request it
9 honors, but a controller may deny an opt-out request if the controller
10 has a good faith, reasonable and documented belief that such request is
11 fraudulent. If a controller denies an opt-out request because the
12 controller believes such request is fraudulent, the controller shall send
13 a notice to the person who made such request disclosing that such
14 controller believes such request is fraudulent, why such controller
15 believes such request is fraudulent and that such controller shall not
16 comply with such request.

17 f. A controller shall establish a process for a consumer to appeal the
18 controller's refusal to take action on a request within a reasonable
19 period of time after the consumer's receipt of the decision. The appeal
20 process shall be conspicuously available and similar to the process for
21 submitting requests to initiate action pursuant to this section. Not later
22 than 45 days after receipt of an appeal, a controller shall inform the
23 consumer in writing of any action taken or not taken in response to the
24 appeal, including a written explanation of the reasons for the decisions.
25 If the appeal is denied, the controller shall also provide the consumer
26 with an online mechanism, if available, or other method through which
27 the consumer may contact the Division of Consumer Affairs in the
28 Department of Law and Public Safety to submit a complaint.

29

30 5. A controller shall be prohibited from discriminating against a
31 consumer if the consumer chooses to opt out of the processing for
32 sale, targeted advertising, or profiling in furtherance of decisions
33 that produce legal or similarly significant effects of the consumer's
34 personal data pursuant to P.L. , c. (C.) (pending before the
35 Legislature as this bill). The provisions of this section shall not
36 prohibit the controller's ability to offer consumers discounts, loyalty
37 programs, or other incentives for the sale of the consumer's personal
38 data, or to provide different services to consumers that are
39 reasonably related to the value of the relevant data, provided that
40 the controller has clearly and conspicuously disclosed to the
41 consumer that the offered discounts, programs, incentives, or
42 services include the sale or processing of personal data that the
43 consumer otherwise has a right to opt out of.

44

45 6. A waiver of the requirements of, or an agreement that does
46 not comply with, the provisions of P.L. , c. (C.) (pending
47 before the Legislature as this bill) shall be void and unenforceable.

1 7. a. A consumer shall have the right to:

2 (1) confirm whether a controller processes the consumer's
3 personal data and accesses such personal data, provided that
4 nothing in this paragraph shall require a controller to provide the
5 data to the consumer in a manner that would reveal the controller's
6 trade secrets;

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

10 (3) delete personal data concerning the consumer;

11 (4) obtain a copy of the consumer's personal data held by the
12 controller in a portable and, to the extent technically feasible,
13 readily usable format that allows the consumer to transmit the data
14 to another entity without hindrance, provided that nothing in this
15 paragraph shall require a controller to provide the data to the
16 consumer in a manner that would reveal the controller's trade
17 secrets; and

18 (5) opt out of the processing of personal data for the purposes of
19 (a) targeted advertising; (b) the sale of personal data; or (c)
20 profiling in furtherance of decisions that produce legal or similarly
21 significant effects concerning the consumer.

22 b. A controller that has lawfully obtained personal data about a
23 consumer from a source other than the consumer shall be deemed in
24 compliance with a consumer's request to delete such data pursuant
25 to this subsection by:

26 (1) retaining a record of the deletion request and the minimum
27 data necessary for the purpose of ensuring the consumer's personal
28 data remains deleted from the controller's records and not using
29 such retained information for any other purpose pursuant to the
30 provisions of P.L. , c. (C.) (pending before the Legislature
31 as this bill); or

32 (2) deleting such personal data.

33

34 8. a. A consumer may designate another person to serve as the
35 consumer's authorized agent and act on the consumer's behalf to
36 opt out of the processing and sale of the consumer's personal data.
37 A consumer may designate an authorized agent using technology,
38 including a link to an Internet website, an Internet browser setting
39 or extension, or a global setting on an electronic device, that allows
40 the consumer to indicate the consumer's intent to opt-out of the
41 collection and processing for the purpose of any sale of data or for
42 the purpose of targeted advertising or for profiling in furtherance of
43 decisions that produce legal or similarly significant effects
44 concerning a consumer. A controller shall comply with an opt-out
45 request received from an authorized agent under this subsection if
46 the controller is able to verify, with commercially reasonable effort,
47 the identity of the consumer and the authorized agent's authority to
48 act on the consumer's behalf.

1 b. (1) Beginning not later than four months following the
2 effective date of P.L. , c. (C.) (pending before the
3 Legislature as this bill), a controller that processes personal data for
4 purposes of targeted advertising, the sale of personal data, or
5 profiling in furtherance of decisions that produce legal or similarly
6 significant effects concerning a consumer shall allow consumers to
7 exercise the right to opt-out of such processing through a user-
8 selected universal opt-out mechanism.

9 (2) The platform, technology, or mechanism shall:

10 (a) not permit its manufacturer to unfairly disadvantage another
11 controller;

12 (b) not make use of a default setting that opts-in a consumer to
13 the processing or sale of personal data, unless the controller has
14 determined that the consumer has selected such default setting and
15 the selection clearly represents the consumer's an affirmative,
16 freely given, and unambiguous choice to opt-out of any processing
17 of such consumer's personal data pursuant to P.L. , c. (C.)
18 (pending before the Legislature as this bill);

19 (c) be consumer-friendly, clearly described, and easy to use by
20 the average consumer;

21 (d) be as consistent as possible with any other similar platform,
22 technology, or mechanism required by any federal or state law or
23 regulation; and

24 (e) enable the controller to accurately determine whether the
25 consumer is a resident of this State and whether the consumer has
26 made a legitimate request to opt out of the processing of personal
27 data for the purposes of any sale of such consumer's personal data
28 or targeted advertising; and

29 (3) Controllers shall inform consumers about the opt-out choices
30 available under P.L. , c. (C.) (pending before the
31 Legislature as this bill).

32 c. The Division of Consumer Affairs in the Department of Law
33 and Public Safety may adopt rules and regulations that detail the
34 technical specifications for one or more universal opt-out
35 mechanisms that clearly communicate a consumer's affirmative,
36 freely given, and unambiguous choice to opt out of the processing
37 of personal data pursuant to P.L. , c. (C.) (pending before
38 the Legislature as this bill), including regulations that permit the
39 controller to accurately authenticate the consumer as a resident of
40 this state and determine that the mechanism represents a legitimate
41 request to opt out of the processing of personal data pursuant to
42 P.L. , c. (C.) (pending before the Legislature as this bill).
43 The division may update the rules that detail the technical
44 specifications for the mechanisms from time to time to reflect the
45 means by which consumers interact with controllers.

1 9. a. A controller shall:

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

5 (2) except as otherwise provided in P.L. , c. (C.)
6 (pending before the Legislature as this bill), not process personal
7 data for purposes that are neither reasonably necessary to, nor
8 compatible with, the purposes for which such personal data is
9 processed, as disclosed to the consumer, unless the controller
10 obtains the consumer's consent;

11 (3) take reasonable measures to establish, implement, and
12 maintain administrative, technical, and physical data security
13 practices to protect the confidentiality, integrity, and accessibility of
14 personal data and to secure personal data during both storage and
15 use from unauthorized acquisition. The data security practices shall
16 be appropriate to the volume and nature of the personal data at
17 issue;

18 (4) not process sensitive data concerning a consumer without
19 first obtaining the consumer's consent, or, in the case of the
20 processing of personal data concerning a known child, without
21 processing such data in accordance with COPPA;

22 (5) not process personal data in violation of the laws of this State
23 and federal laws that prohibit unlawful discrimination against
24 consumers;

25 (6) provide an effective mechanism for a consumer to revoke the
26 consumer's consent under this section that is at least as easy as the
27 mechanism by which the consumer provided the consumer's
28 consent and, upon revocation of such consent, cease to process the
29 data as soon as practicable, but not later than 15 days after the
30 receipt of such request;

31 (7) not process the personal data of a consumer for purposes of
32 targeted advertising, the sale of the consumer's personal data, or
33 profiling in furtherance of decisions that produce legal or similarly
34 significant effects concerning a consumer without the consumer's
35 consent, under circumstances where a controller has actual
36 knowledge, or willfully disregards, that the consumer is at least 13
37 years of age but younger than 17 years of age;

38 (8) specify the express purposes for which personal data are
39 processed; and

40 (9) not conduct processing that presents a heightened risk of
41 harm to a consumer without conducting and documenting a data
42 protection assessment of each of its processing activities that
43 involve personal data acquired on or after the effective date of
44 P.L. , c. (C.) (pending before the Legislature as this bill)
45 that present a heightened risk of harm to a consumer.

46 b. Data protection assessments shall identify and weigh the
47 benefits that may flow, directly and indirectly, from the processing
48 to the controller, the consumer, other stakeholders, and the public

1 against the potential risks to the rights of the consumer associated
2 with the processing, as mitigated by safeguards that the controller
3 can employ to reduce the risks. The controller shall factor into this
4 assessment the use of de-identified data and the reasonable
5 expectations of consumers, as well as the context of the processing
6 and the relationship between the controller and the consumer whose
7 personal data will be processed. A controller shall make the data
8 protection assessment available to the Division of Consumer Affairs
9 in the Department of Law and Public Safety upon request. The
10 division may evaluate the data protection assessment for
11 compliance with the duties contained in this section and with other
12 laws. Data protection assessments shall be confidential and exempt
13 from public inspection under P.L.1963 c.3 (C.47:1A-1 et al.). The
14 disclosure of a data protection assessment pursuant to a request
15 from the division under this section shall not constitute a waiver of
16 any attorney-client privilege or work-product protection that might
17 otherwise exist with respect to the assessment and any information
18 contained in the assessment.

19 c. For the purposes of this section, “heightened risk” includes:

20 (1) processing personal data for purposes of targeted advertising
21 or for profiling if the profiling presents a reasonably foreseeable
22 risk of: unfair or deceptive treatment of, or unlawful disparate
23 impact on, consumers; financial or physical injury to consumers; a
24 physical or other intrusion upon the solitude or seclusion, or the
25 private affairs or concerns, of consumers if the intrusion would be
26 offensive to a reasonable person; or other substantial injury to
27 consumers;

28 (2) selling personal data; and

29 (3) processing sensitive data.

30

31 10. Nothing in P.L. , c. (C.) (pending before the
32 Legislature as this bill) shall apply to:

33 a. protected health information collected by a covered entity or
34 business associate subject to the privacy, security, and breach
35 notification rules issued by the United States Department of Health
36 and Human Services, Parts 160 and 164 of Title 45 of the Code of
37 Federal Regulations, established pursuant to the "Health Insurance
38 Portability and Accountability Act of 1996," Pub.L.104-191, and
39 the “Health Information Technology for Economic and Clinical
40 Health Act,” 42 U.S.C. s.17921 et seq.;

41 b. a financial institution or an affiliate of a financial institution
42 that is subject to Title V of the federal “Gramm-Leach-Bliley Act,”
43 15 U.S.C. s.6801 et seq., and the rules and implementing
44 regulations promulgated thereunder;

45 c. the secondary market institutions identified in
46 15 U.S.C. s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii);

47 d. an insurance institution subject to P.L.1985, c.179
48 (C.17:23A-1 et seq.);

- 1 e. the sale of a consumer’s personal data by the New Jersey
2 Motor Vehicle Commission that is permitted by the federal
3 "Drivers' Privacy Protection Act of 1994," 18 U.S.C. s.2721 et seq.;
- 4 f. personal data collected, processed, sold, or disclosed by a
5 consumer reporting agency, as defined in 15 U.S.C. s.1681a(f), if
6 the collection, processing, sale, or disclosure of the personal data is
7 limited, governed, and collected, maintained, disclosed, sold,
8 communicated, or used only as authorized by the federal “Fair
9 Credit Reporting Act,” 15 U.S.C. s.1681 et seq., and implementing
10 regulations;
- 11 g. any State agency as defined in section 2 of P.L.1971, c.182
12 (C.52:13D-13), any political subdivision, and any division, board,
13 bureau, office, commission, or other instrumentality created by a
14 political subdivision; or
- 15 h. personal data that is collected, processed, or disclosed, as
16 part of research conducted in accordance with the Federal Policy for
17 the protection of human subjects pursuant to 45 C.F.R. Part 46 or
18 the protection of human subjects pursuant to 21 C.F.R. Parts 50 and
19 56.
- 20
- 21 11. Nothing in P.L. , c. (C.) (pending before the
22 Legislature as this bill) shall require an operator to:
- 23 a. re-identify de-identified data;
- 24 b. collect, retain, use, link, or combine personal data
25 concerning a consumer that it would not otherwise collect, retain,
26 use, link, or combine in the ordinary course of business.
- 27
- 28 12. a. Nothing in P.L. , c. (C.) (pending before the
29 Legislature as this bill) shall be construed to restrict a controller’s
30 or processor’s ability to:
- 31 (1) comply with federal or State law or regulations;
- 32 (2) comply with a civil, criminal or regulatory inquiry,
33 investigation, subpoena or summons by federal, State, municipal or
34 other governmental authorities;
- 35 (3) cooperate with law enforcement agencies concerning conduct
36 or activity that the controller or processor reasonably and in good
37 faith believes may violate federal, State or municipal ordinances or
38 regulations;
- 39 (4) investigate, establish, exercise, prepare for or defend legal
40 claims;
- 41 (5) provide a product or service specifically requested by a
42 consumer;
- 43 (6) perform under a contract to which a consumer is a party,
44 including fulfilling the terms of a written warranty;
- 45 (7) take steps at the request of a consumer prior to entering into a
46 contract;
- 47 (8) take immediate steps to protect an interest that is essential for
48 the life or physical safety of the consumer or another individual,

- 1 and where the processing cannot be manifestly based on another
2 legal basis;
- 3 (9) prevent, detect, protect against or respond to security
4 incidents, identity theft, fraud, harassment, malicious or deceptive
5 activities or any illegal activity, preserve the integrity or security of
6 systems or investigate, report or prosecute those responsible for any
7 such action;
- 8 (10) engage in public or peer-reviewed scientific or statistical
9 research in the public interest that adheres to all other applicable
10 ethics and privacy laws and is approved, monitored and governed
11 by an institutional review board that determines, or similar
12 independent oversight entities that determine,
- 13 (a) whether the deletion of the information is likely to provide
14 substantial benefits that do not exclusively accrue to the controller,
15 (b) the expected benefits of the research outweigh the privacy
16 risks, and
17 (c) whether the controller has implemented reasonable
18 safeguards to mitigate privacy risks associated with research,
19 including any risks associated with re-identification;
- 20 (11) assist another controller, processor, or third party with any
21 of the obligations under P.L. , c. (C.) (pending before the
22 Legislature as this bill); or
- 23 (12) personal data for reasons of public interest in the area of
24 public health, community health, or population health, but solely to
25 the extent that such processing is
- 26 (a) subject to suitable and specific measures to safeguard the
27 rights of the consumer whose personal data is being processed, and
28 (b) under the responsibility of a professional subject to
29 confidentiality obligations under federal, State or local law.
- 30 b. The obligations imposed on controllers or processors under
31 P.L. , c. (C.) (pending before the Legislature as this bill)
32 shall not restrict a controller's or processor's ability to collect, use or
33 retain data for internal use to:
- 34 (1) conduct internal research to develop, improve, or repair
35 products, services, or technology;
- 36 (2) effectuate a product recall;
- 37 (3) identify and repair technical errors that impair existing or
38 intended functionality; or
- 39 (4) perform internal operations that are reasonably aligned with
40 the expectations of the consumer or reasonably anticipated based on
41 the consumer's existing relationship with the controller, or are
42 otherwise compatible with processing data in furtherance of the
43 provision of a product or service specifically requested by a
44 consumer or the performance of a contract to which the consumer is
45 a party. Personal data collected, used, or retained pursuant to this
46 subsection shall, where applicable, take into account the nature and
47 purpose or purposes of such collection, use or retention. Such data
48 shall be subject to reasonable administrative, technical, and physical

1 measures to protect the confidentiality, integrity, and accessibility
2 of the personal data and to reduce reasonably foreseeable risks of
3 harm to consumers relating to such collection, use, or retention of
4 personal data.

5 c. The obligations imposed on controllers or processors under
6 P.L. , c. (C.) (pending before the Legislature as this bill)
7 shall not apply where compliance by the controller or processor
8 with the provisions of law would violate an evidentiary privilege
9 under the laws of this State. Nothing in P.L. , c. (C.)
10 (pending before the Legislature as this bill) shall be construed to
11 prevent a controller or processor from providing personal data
12 concerning a consumer to a person covered by an evidentiary
13 privilege under the laws of the State as part of a privileged
14 communication.

15 d. Personal data that are processed by a controller pursuant to an
16 exception provided by this section:

17 (1) shall not be processed for any purpose other than a purpose
18 expressly listed in this section; and

19 (2) shall be processed solely to the extent that the processing is
20 necessary, reasonable, and proportionate to the specific purpose or
21 purposes listed in this section.

22 e. If a controller processes personal data pursuant to an
23 exemption in this section, the controller bears the burden of
24 demonstrating that such processing qualifies for the exemption and
25 complies with the requirements in this section.

26 f. Processing personal data for the purposes expressly identified
27 in this section shall not solely make a legal entity a controller with
28 respect to such processing if such entity would not otherwise meet
29 the definition of a controller.

30
31 13. a. Controllers and processors shall meet their respective
32 obligations established under P.L. , c. (C.) (pending before
33 the Legislature as this bill).

34 b. Processors shall adhere to the instructions of the controller
35 and assist the controller to meet its obligations under this act.
36 Taking into account the nature of processing and the information
37 available to the processor, the processor shall assist the controller
38 by:

39 (1) taking appropriate technical and organizational measures,
40 insofar as possible, for the fulfillment of the controller's obligation
41 to respond to consumer requests to exercise their rights under this
42 act;

43 (2) helping to meet the controller's obligations in relation to the
44 security of processing the personal data and in relation to
45 notification of a breach of the security of the system; and

46 (3) providing information to the controller necessary to enable
47 the controller to conduct and document any data protection
48 assessments required by section 9 of P.L. , c. (C.)

1 (pending before the Legislature as this bill). The controller and
2 processor are each responsible for only the measures allocated to
3 them.

4 c. Notwithstanding the instructions of the controller, a
5 processor shall:

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

8 (2) engage a subcontractor pursuant to a written contract in
9 accordance with subsection e. of this section that requires the
10 subcontractor to meet the obligations of the processor with respect
11 to the personal data.

12 d. Taking into account the context of processing, the controller
13 and the processor shall implement appropriate technical and
14 organizational measures to ensure a level of security appropriate to
15 the risk and establish a clear allocation of the responsibilities
16 between them to implement the measures.

17 e. Processing by a processor shall be governed by a contract
18 between the controller and the processor that is binding on both
19 parties and that sets forth:

20 (1) the processing instructions to which the processor is bound,
21 including the nature and purpose of the processing;

22 (2) the type of personal data subject to the processing, and the
23 duration of the processing;

24 (3) the requirements imposed by this subsection and subsections
25 c. and d. of this section; and

26 (4) the following requirements:

27 (a) At the discretion of the controller, the processor shall delete
28 or return all personal data to the controller as requested at the end of
29 the provision of services, unless retention of the personal data is
30 required by law;

31 (b) (i) The processor shall make available to the controller all
32 information necessary to demonstrate compliance with the
33 obligations in this act; and

34 (ii) The processor shall allow for, and contribute to, reasonable
35 assessments and inspections by the controller or the controller's
36 designated assessor. Alternatively, the processor may, with the
37 controller's consent, arrange for a qualified and independent
38 assessor to conduct, at least annually and at the processor's expense,
39 an assessment of the processor's policies and technical and
40 organizational measures in support of the obligations under this act
41 using an appropriate and accepted control standard or framework
42 for the assessment as applicable. The processor shall provide a
43 report of the assessment to the controller upon request.

44 f. In no event may a contract relieve a controller or a processor
45 from the liabilities imposed on them by virtue of its role in the
46 processing relationship as defined by P.L. , c. (C.)
47 (pending before the Legislature as this bill).

1 g. Determining whether a person is acting as a controller or
2 processor with respect to a specific processing of data shall be a
3 fact-based determination that depends upon the context in which
4 personal data are to be processed. A person that is not limited in its
5 processing of personal data pursuant to a controller's instructions, or
6 that fails to adhere to the instructions, shall be deemed a controller
7 and not a processor with respect to a specific processing of data. A
8 processor that continues to adhere to a controller's instructions with
9 respect to a specific processing of personal data shall remain a
10 processor. If a processor begins, alone or jointly with others,
11 determining the purposes and means of the processing of personal
12 data, it shall be deemed a controller with respect to the processing.

13

14 14. a. It shall be an unlawful practice and violation of P.L.1960,
15 c.39 (C.56:8-1 et seq.) for a controller to violate the provisions of
16 P.L. , c. (C.) (pending before the Legislature as this bill).

17 b. Until the first day of the 18th month next following the
18 effective date of P.L. , c. (C.) (pending before the
19 Legislature as this bill), prior to bringing an enforcement action
20 before an administrative law judge or a court of competent
21 jurisdiction in this State, the Division of Consumer Affairs in the
22 Department of Law and Public Safety shall issue a notice to the
23 controller if a cure is deemed possible. If the operator controller
24 fails to cure the alleged violation of P.L. , c. (C.) (pending
25 before the Legislature as this bill) within 30 days after receiving
26 notice of alleged noncompliance from the division, such
27 enforcement action may be brought.

28

29 15. The Director of the Division of Consumer Affairs in the
30 Department of Law and Public Safety shall promulgate rules and
31 regulations, pursuant to the "Administrative Procedure Act,"
32 P.L.1968, c.410 (C.52:14B-1 et seq.), necessary to effectuate the
33 purposes of P.L. , c. (C.) (pending before the Legislature as
34 this bill).

35

36 16. The Office of the Attorney General shall have sole and
37 exclusive authority to enforce a violation of P.L. , c. (C.)
38 (pending before the Legislature as this bill). Nothing in
39 P.L. , c. (C.) (pending before the Legislature as this bill)
40 shall be construed as providing the basis for, or subject to, a private
41 right of action for violations of P.L. , c. (C.) (pending before
42 the Legislature as this bill) or under any other law.

43

44 17. This act shall take effect on the 365th day following the date
45 of enactment, except that the Director of the Division of Consumer
46 Affairs may take any anticipatory administrative action in advance as
47 shall be necessary for the implementation of this act.

STATEMENT

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48

This bill imposes requirements on certain entities (i.e., controllers) that determine the purposes and means of processing personal data. However, the provisions of the bill would only apply to controllers, which conduct business in the State or produce products or services that are targeted to residents of the State, and which control or process the personal data of a minimum number of consumers each year.

The bill requires a controller to provide notice to consumers of the collection and disclosure of “personal data,” as that term is defined in the bill, to third parties. The bill also sets forth various requirements concerning the information that is required to be included in this notice. The bill also imposes other requirements and limitations on controllers regarding the processing of personal data, including limiting the collection and processing of personal data, taking reasonable measures to protect personal data, and obtaining consumer consent before processing certain data. Specifically, the bill imposes additional restrictions on the processing of sensitive data, as defined in the bill, or the processing of a child’s personal data.

Additionally, the bill requires a controller that processes personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer to allow consumers to exercise the right to opt-out of such processing through a user-selected universal opt-out mechanism. The bill permits a consumer to authorize another person to act on the consumer’s behalf to opt out of the sale of personal data. The bill prohibits a controller from discriminating against a consumer if the consumer chooses to opt out of the processing for sale, targeted advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects of the consumer’s personal data, provided certain exceptions.

The bill requires a controller to complete data protection assessments, as described in the bill, and to make such assessments available to the Division of Consumer Affairs.

The bill provides that a processor, in addition to a controller, has certain duties under the bill. A processor is required to cooperate with a controller so that a controller remains in compliance with the bill.

Under the bill, the consumers of a controller may submit a verified request to exercise any rights established under the bill. The bill requires a controller to respond to each verified request within 45 days, except as extended in certain circumstances. Any information provided in response to a verified request would be provided free of charge, except that a controller may charge a fee for a second or subsequent request submitted within a 12-month

1 period. The bill also requires a controller to establish a process for
2 consumers to appeal the controller's refusal to take action on a
3 request.
4 The bill also establishes certain consumer rights concerning
5 personal data, including the right to: confirm whether a controller
6 may process or access the consumer's personal data; correct
7 inaccuracies in the consumer's personal data; delete personal data
8 concerning the consumer; obtain a copy of the consumer's personal
9 data held by the controller in a portable format; and opt out of the
10 processing of personal data for the purposes of (i) targeted
11 advertising; (ii) the sale of personal data; or (iii) profiling in
12 furtherance of decisions that produce legal or similarly significant
13 effects concerning the consumer.

WITHDRAWN