SENATE, No. 332

STATE OF NEW JERSEY

220th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2022 SESSION

Sponsored by:
Senator TROY SINGLETON
District 7 (Burlington)
Senator RICHARD J. CODEY
District 27 (Essex and Morris)
Assemblyman RAJ MUKHERJI
District 33 (Hudson)
Assemblyman DANIEL R. BENSON
District 14 (Mercer and Middlesex)
Assemblyman PAUL D. MORIARTY
District 4 (Camden and Gloucester)

Co-Sponsored by:
Senators Greenstein, Madden, Pou, Assemblywoman McKnight,
Assemblymen DeAngelo, Verrelli and Wimberly

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

CURRENT VERSION OF TEXT
As amended by the General Assembly on December 21, 2023.

(Sponsorship Updated As Of: 1/8/2024)
AN ACT concerning commercial Internet websites, consumers, and personally identifiable information and supplementing Title 56 of the Revised Statutes.

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

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

“Affiliate” means a legal entity that controls, is controlled by, or is under common control with another legal entity.

“Business” means 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, that collects consumers’ personal information. “Business” does not include non-profit organizations.

“Commercial Internet website” means a website operated for business purposes, including, but not limited to, the sale of goods and services, which collects and maintains personally identifiable information from a consumer.

“Consumer” means an identified person who is a resident of this State acting only in an individual, job seeking, or household context. “Consumer” shall not include a person otherwise acting in a commercial or employment context.

“De-identified data” means: data that cannot be linked to a consumer without additional information that is kept separately; or data that has been modified to a degree that the risk of re-identification, consistent with guidance from the Federal Trade Commission and the National Institute of Standards and Technology, is small, as determined by the Director of the Division of Consumer Affairs in the Department of Law and Public Safety pursuant to section 8 of P.L. , c. (C. ) (pending before the Legislature as this bill), that is subject to a public commitment by the operator not to attempt to re-identify the data, and to which one or more enforceable controls to prevent re-identification has been applied, which may include legal, administrative, technical, or contractual controls.

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

EXPLANATION – Matter enclosed in bold-faced brackets [thus] in the above bill is not enacted and is intended to be omitted in the law.

Matter underlined thus is new matter.
Matter enclosed in superscript numerals has been adopted as follows:
Senate floor amendments adopted August 5, 2022.
Senate floor amendments adopted November 21, 2022.
Senate floor amendments adopted December 19, 2022.
Assembly AST committee amendments adopted May 11, 2023.
Assembly AJU committee amendments adopted December 18, 2023.
Assembly floor amendments adopted December 21, 2023.
“Disclose” means to release, transfer, share, disseminate, make available, or otherwise communicate orally, or in writing, or by electronic or any other means by an operator to a third party a consumer’s personally identifiable information. “Disclose” shall not include:

- the disclosure of a consumer’s personally identifiable information by an operator to a third party under a written contract authorizing the third party to use the personally identifiable information to perform services on behalf of the operator, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying consumer information, processing payments, providing financing, or similar services, but only if the contract prohibits the third party from using the personally identifiable information for any reason other than performing the specified service on behalf of the operator and from disclosing personally identifiable information to additional third parties unless expressly authorized by the consumer;
- the disclosure of personally identifiable information by an operator to a third party based on a good-faith belief that disclosure is required to comply with applicable law, regulation, legal process, or court order;
- the disclosure of personally identifiable information by an operator to a third party that is reasonably necessary to address fraud, risk management, security, or technical issues, to protect the operator’s rights or property, or to protect a consumer or the public from illegal activities as required by law; or
- the disclosure of personally identifiable information by an operator to a third party in connection with the proposed or actual sale or merger of the operator, or sale of all or part of its assets, to a third party.

“Online service” means any service provided over the Internet that collects and maintains personally identifiable information from a consumer.

“Operator” means a person or entity that operates a commercial Internet website or an online service, and includes any third party that tracks or collects any information concerning a customer’s usage of a commercial Internet website, regardless of whether the third party owns or operates the website. “Operator” shall not include any third party that operates, hosts, or manages, but does not own, a commercial Internet website or online service on the operator’s behalf, or processes information on behalf of the operator.

“Personally identifiable information” means any information that is linked or reasonably linkable to an identified or identifiable person.

“Personally identifiable information” shall not include de-identified data or publicly available information.

“Publicly available information” means information that is lawfully made available from federal, State, or local government...
“Publicly available information” means information that is lawfully made available from federal, State, or local government records, or widely-distributed media.

“Sale” means the exchange of personally identifiable information for monetary consideration by the operator to a third party for purposes of licensing or selling personally identifiable information at the third party's discretion to additional third parties. "Sale" shall not include the following:

- the disclosure of personally identifiable information to a service provider that processes that information on behalf of the operator;
- the disclosure of personally identifiable information to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personally identifiable information to the operator;
- the disclosure or transfer of personally identifiable information to an affiliate of the operator; or
- the disclosure or transfer of personally identifiable information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the operator’s assets.

“Service provider” means a person, private entity, public entity, agency, or other entity that processes personally identifiable information on behalf of the operator and who shall provide sufficient guarantees to the operator to implement appropriate technical and organizational measures in a manner that processing shall ensure the protection of the consumer’s personally identifiable information.

“Third party” means a person, private entity, public entity, agency, or entity other than the consumer, operator, or affiliate or service provider of the operator.

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

2. a. An operator that collects the personally identifiable information of a consumer through a commercial Internet website or an online service shall provide on its commercial Internet website or an online service notification to a consumer that shall include, but not be limited to:

(1) the categories of the personally identifiable information that the operator collects through the commercial Internet website
or online service about a consumer who uses or visits the operator’s commercial Internet website or online service;

(2) the categories of all third parties with which the operator may disclose a consumer’s personally identifiable information;

(3) whether a third party may collect personally identifiable information about a consumer’s online activities over time and across different commercial Internet websites or online services when the consumer uses the Internet website or online service of the operator;

(4) a description of the process for an individual consumer who uses or visits the commercial Internet website or online service to review and request changes to any of the consumer’s personally identifiable information that is collected by the commercial Internet website or online service of the operator;

(5) the process by which the operator notifies consumers who use or visit the commercial Internet website or online service of material changes to the notification required to be made available pursuant to this subsection, along with the effective date of the notice; and

(6) information concerning one or more designated request addresses of the operator.

b. In addition to the requirements of subsection a. of this section, an operator shall include the notification as a separate section of the operator’s privacy policy.

c. (1) The process described in paragraph (4) of subsection a. of this section shall consist of one or more methods for submitting requests to the operator. The operator shall provide a toll-free phone number, email address, or both, for the submission of requests by a customer to review or change personally identifiable information. The consumer shall submit verified documents supporting the consumer’s request to change personally identifiable information. The operator shall take steps to promptly verify the data and reply to the consumer’s request.

(2) An operator may deny an individual consumer’s request to change the consumer’s personally identifiable information if:

(a) the operator is legally obligated to retain the personally identifiable information; or

(b) the changes cannot be verified through the submitted documentation.

3. a. An operator that collects a consumer’s personally identifiable information through its commercial Internet website or online service and discloses the consumer’s personally identifiable information to a third party shall make the following
information available to the consumer free of charge upon receipt of
a verified request from the consumer for this information through a
designated request address:
   (1) the category or categories of a consumer’s personally
       identifiable information that were disclosed; and
   (2) the category or categories of the third parties that received the
       consumer’s personally identifiable information.

b. An operator that receives a verified request from a consumer
   pursuant to subsection a. of this section shall provide a response to
   the consumer within 60 days of the operator’s verification of the
   request and shall provide the information, pursuant to subsection a.
   of this section, for all disclosures of personally identifiable
   information that occurred in the prior 12 months.

c. This section shall not apply to personally identifiable
   information disclosed prior to the effective date of P.L. , c.
   (C. ) (pending before the Legislature as this bill). *This section
   shall not apply to personally identifiable information collected prior
   to the effective date of P.L. , c. (C. ) (pending before the
   Legislature as this bill) unless the controller continues to store such
   information thereafter. *This section

§4. a. An operator that collects the personally identifiable
information of a consumer through its [commercial Internet website
or] online service and sells the personally identifiable information
of the consumer [through the Internet] shall clearly and
conspicuously post a link, on its [commercial Internet website or]
online service or in another prominently accessible location the
[commercial Internet website] online service maintains for
consumer privacy settings, to an Internet webpage maintained by the
operator, which enables a consumer, by verified request, to opt [out
of] into the sale of the consumer’s personally identifiable
information. The method in which a consumer may opt [out] in
shall be in a form and manner determined by the operator, provided
that a consumer shall not be required to establish an account with
the operator in order to opt [out of] into the sale of a consumer’s
personally identifiable information.
b. An operator shall be prohibited from discriminating against
a consumer if the consumer chooses to opt out of the sale of the
consumer’s personally identifiable information pursuant to
subsection a. of this section. The provisions of this section shall not
prohibit the operator’s ability to offer consumers discounts, loyalty
programs, or other incentives for the sale of the consumer’s
personally identifiable information, or to provide different services
to consumers that are reasonably related to the value of the relevant
data*, provided that the operator has clearly and conspicuously
disclosed to the consumer that the offered discounts, programs,
incentives, or services require consenting to the sale or processing
of personally identifiable information that the consumer otherwise has a right to opt out of.\(^5\)

\(^5\) A waiver of the requirements of, or an agreement that does not comply with, the provisions of P.L. 1960, c. (C. ) (pending before the Legislature as this bill) shall be void and unenforceable.\(^5\)

\(^5\) Nothing in P.L. 1960, c. (C. ) (pending before the Legislature as this bill) shall apply to:

a. protected health information collected by a covered entity or business associate subject to the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the "Health Insurance Portability and Accountability Act of 1996," Pub.L.104-191, and the "Health Information Technology for Economic and Clinical Health Act," \(^4\)42 U.S.C. s.17921 et seq.\(^4\)

b. a financial institution or an affiliate of a financial institution that is subject to Title V of the federal “Gramm-Leach-Bliley Act \(^4\) of 1999\(^4\),” 15 U.S.C. s.6801 et seq., and the rules and implementing regulations promulgated thereunder;

c. the secondary market institutions identified in 15 U.S.C. s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii); \(^4\)
d. an insurance institution subject to P.L.1985, c.179 (C.17:23A et seq.); \(^4\)
e. the sale of a consumer’s personally identifiable information by the New Jersey Motor Vehicle Commission that is permitted by the federal "Drivers' Privacy Protection Act of 1994," 18 U.S.C. s.2721 et seq.; \(^4\) and \(^4\)
f. personally identifiable information collected, processed, sold, or disclosed by a consumer reporting agency, as defined in 15 U.S.C. s.1681a(f), if the collection, processing, sale, or disclosure of the personally identifiable information is limited by the federal “Fair Credit Reporting Act,” 15 U.S.C. s.1681 et seq., and implementing regulations.\(^5\)

\(^5\) Nothing in P.L. 1960, c. (C. ) (pending before the Legislature as this bill) shall require an operator to:

a. re-identify de-identified data;

b. collect, retain, use, link, or combine personally identifiable information concerning a consumer that it would not otherwise collect, retain, use, link, or combine in the ordinary course of business.\(^5\)

\(^5\) It shall be an unlawful practice and violation of P.L.1960, c.39 (C.56:8-1 et seq.) for an operator to fail to notify a consumer of
the sale of personally identifiable information pursuant to sections 2 and 3 of P.L.  (C. ) (pending before the Legislature as this bill) or fail to allow a consumer to opt out of the sale of a consumer’s personally identifiable information pursuant to section 4 of P.L.  (C. ) (pending before the Legislature as this bill) if the operator fails to cure any alleged violation of P.L.  (C. ) (pending before the Legislature as this bill) within 30 days after receiving notice of alleged noncompliance from the Attorney General.  

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

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

11. This act shall take effect on the 180th day following the date of enactment, except that the Director of the Division of Consumer Affairs may take any anticipatory administrative action in advance as shall be necessary for the implementation of this act.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- The disclosure of personal data to a processor that processes the personal data on the controller’s behalf;
- The disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer;
- The disclosure or transfer of personal data to an affiliate of the controller;
- The disclosure of personal data that the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience; or
- The disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition,
bankruptcy, or other transaction in which the third party assumes
control of all or part of the controller’s assets.

“Sensitive data” means personal data revealing racial or ethnic
origin; religious beliefs; mental or physical health condition, treatment,
or diagnosis; financial information, which shall include a consumer’s
account number, account log-in, financial account, or credit or debit
card number, in combination with any required security code, access
code, or password that would permit access to a consumer’s financial
account; sex life or sexual orientation; citizenship or immigration
status; status as transgender or non-binary; genetic or biometric data
that may be processed for the purpose of uniquely identifying an
individual; personal data collected from a known child; or precise
geolocation data.

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

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

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

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

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

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

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

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

1. the categories of the personal data that the controller processes;
2. the purpose for processing personal data;
3. the categories of all third parties to which the controller may disclose a consumer’s personal data;
4. the categories of personal data that the controller shares with third parties, if any;
5. how consumers may exercise their consumer rights, including the controller’s contact information and how a consumer may appeal a controller’s decision with regard to the consumer’s request;
6. the process by which the controller notifies consumers of material changes to the notification required to be made available pursuant to this subsection, along with the effective date of the notice; and
7. an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

b. If a controller sells personal data to third parties or processes personal data for the 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, the controller shall clearly and conspicuously disclose such sale or processing, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing, a description of the process for a consumer to review and make requests pursuant to section 4 of this act, P.L., c. (C.) (pending before the Legislature as this bill) §. 

c. A controller shall not:

1. require a consumer to create a new account in order to exercise a right, but may require a consumer to use an existing account to submit a verified request; or
2. based solely on the exercise of a right and unrelated to feasibility or the value of a service, increase the cost of, or decrease the availability of, the product or service. 

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

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

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

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

e. If a controller is unable to authenticate a request to exercise any of the rights afforded under section 5 of P.L. c. (C. ) (pending before the Legislature as this bill) using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request , but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent and that such controller shall not comply with such request.

f. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than 45 days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer
with an online mechanism, if available, or other method through which
the consumer may contact the Division of Consumer Affairs in the
Department of Law and Public Safety to submit a complaint.\(^5\)

5. A controller shall be prohibited 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 pursuant to P.L. \(\ldots\) (pending before the
Legislature as this bill). The provisions of this section shall not
prohibit the controller’s ability to offer consumers discounts, loyalty
programs, or other incentives for the sale of the consumer’s personal
data, or to provide different services to consumers that are
reasonably related to the value of the relevant data, provided that
the controller has clearly and conspicuously disclosed to the
consumer that the offered discounts, programs, incentives, or
services include the sale or processing of personal data that the
consumer otherwise has a right to opt out of.\(^5\)

6. A waiver of the requirements of, or an agreement that does
not comply with, the provisions of P.L. \(\ldots\) (pending
before the Legislature as this bill) shall be void and unenforceable.\(^5\)

7. a. A consumer shall have the right to:
(1) confirm whether a controller processes the consumer’s
personal data and accesses such personal data, provided that
nothing in this paragraph shall require a controller to provide the
data to the consumer in a manner that would reveal the controller’s
trade secrets;
(2) correct inaccuracies in the consumer’s personal data, taking
into account the nature of the information and the purposes of the
processing of the information;
(3) delete personal data concerning the consumer;
(4) obtain a copy of the consumer’s personal data held by the
controller in a portable and, to the extent technically feasible,
readily usable format that allows the consumer to transmit the data
to another entity without hindrance, provided that nothing in this
paragraph shall require a controller to provide the data to the
consumer in a manner that would reveal the controller’s trade
secrets; and
(5) opt out of the processing of personal data for the purposes of
(a) targeted advertising; (b) the sale of personal data; or (c)
profiling in furtherance of decisions that produce legal or similarly
significant effects concerning the consumer.

b. A controller that has lawfully obtained personal data about a
consumer from a source other than the consumer shall be deemed in
compliance with a consumer’s request to delete such data pursuant
to this subsection by:
(1) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer’s personal data remains deleted from the controller’s records and not using such retained information for any other purpose pursuant to the provisions of P.L. , c. (C. ) (pending before the Legislature as this bill); or

(2) deleting such personal data.

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

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

(2) The platform, technology, or mechanism shall;

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

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

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

(d) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation; and
(e) enable the controller to accurately determine whether the consumer is a resident of this State and whether the consumer has made a legitimate request to opt out of the processing of personal data for the purposes of any sale of such consumer’s personal data or targeted advertising; and

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

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

9. a. A controller shall:

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

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

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

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

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

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

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

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

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

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

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

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

(2) selling personal data; and

(3) processing sensitive data.
d. A single data protection assessment may address a comparable set of processing operations that include similar activities.⁶

10. Nothing in P.L., c. (C.) (pending before the Legislature as this bill) shall apply to:
a. protected health information collected by a covered entity or business associate subject to the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the "Health Insurance Portability and Accountability Act of 1996," Pub.L.104-191, and the “Health Information Technology for Economic and Clinical Health Act,” 42 U.S.C. s.17921 et seq.;
b. a financial institution, data, or an affiliate of a financial institution that is subject to Title V of the federal “Gramm-Leach-Bliley Act,” 15 U.S.C. s.6801 et seq., and the rules and implementing regulations promulgated thereunder;
c. the secondary market institutions identified in 15 U.S.C. s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii);
d. an insurance institution subject to P.L.1985, c.179 (C.17:23A et seq.);
e. the sale of a consumer’s personal data by the New Jersey Motor Vehicle Commission that is permitted by the federal “Drivers’ Privacy Protection Act of 1994,” 18 U.S.C. s.2721 et seq.;
f. personal data collected, processed, sold, or disclosed by a consumer reporting agency, as defined in 15 U.S.C. s.1681a(f), if the collection, processing, sale, or disclosure of the personal data is limited, governed, and collected, maintained, disclosed, sold, communicated, or used only as authorized by the federal “Fair Credit Reporting Act,” 15 U.S.C. s.1681 et seq., and implementing regulations;
g. any State agency as defined in section 2 of P.L.1971, c.182 (C.52:13D-13), any political subdivision, and any division, board, bureau, office, commission, or other instrumentality created by a political subdivision; or
h. personal data that is collected, processed, or disclosed, as part of research conducted in accordance with the Federal Policy for the protection of human subjects pursuant to 45 C.F.R. Part 46 or the protection of human subjects pursuant to 21 C.F.R. Parts 50 and 56.⁵

11. Nothing in P.L., c. (C.) (pending before the Legislature as this bill) shall require an operator, a controller, to:
a. re-identify de-identified data;
b. collect, retain, use, link, or combine personal data concerning a consumer that it would not otherwise collect, retain, use, link, or combine in the ordinary course of business.
§12. a. Nothing in P.L. [insert number], c. [insert number] (pending before the Legislature as this bill) shall be construed to restrict a controller’s or processor’s ability to:

1. comply with federal or State law or regulations;
2. comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, State, municipal or other governmental authorities;
3. cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, State or municipal ordinances or regulations;
4. investigate, establish, exercise, prepare for or defend legal claims;
5. provide a product or service specifically requested by a consumer;
6. perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
7. take steps at the request of a consumer prior to entering into a contract;
8. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;
9. prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;
10. engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine,
   a. whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller,
   b. the expected benefits of the research outweigh the privacy risks, and
   c. whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;
11. assist another controller, processor, or third party with any of the obligations under P.L. [insert number], c. [insert number] (pending before the Legislature as this bill); or
12. personal data for reasons of public interest in the area of public health, community health, or population health, but solely to the extent that such processing is
   a. subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and
(b) under the responsibility of a professional subject to confidentiality obligations under federal, State or local law.

b. The obligations imposed on controllers or processors under P.L. , c. (pending before the Legislature as this bill) shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to:

1. conduct internal research to develop, improve, or repair products, services, or technology;
2. effectuate a product recall;
3. identify and repair technical errors that impair existing or intended functionality; or
4. perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party. Personal data collected, used, or retained pursuant to this subsection shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

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

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

1. shall not be processed for any purpose other than a purpose expressly listed in this section; and
2. shall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific purpose or purposes listed in this section.

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

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

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

b. Processors shall adhere to the instructions of the controller
and assist the controller to meet its obligations under this act.
Taking into account the nature of processing and the information
available to the processor, the processor shall assist the controller
by:
(1) taking appropriate technical and organizational measures,
insofar as possible, for the fulfillment of the controller's obligation
to respond to consumer requests to exercise their rights under this
act;
(2) helping to meet the controller's obligations in relation to the
security of processing the personal data and in relation to
notification of a breach of the security of the system; and
(3) providing information to the controller necessary to enable
the controller to conduct and document any data protection
assessments required by section 9 of P.L. , c. (C. )
(pending before the Legislature as this bill). The controller and
processor are each responsible for only the measures allocated to
them.

c. Notwithstanding the instructions of the controller, a
processor shall:
(1) ensure that each person processing the personal data is
subject to a duty of confidentiality with respect to the data; and
(2) engage a subcontractor pursuant to a written contract in
accordance with subsection e. of this section that requires the
subcontractor to meet the obligations of the processor with respect
to the personal data.

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

e. Processing by a processor shall be governed by a contract
between the controller and the processor that is binding on both
parties and that sets forth:
(1) the processing instructions to which the processor is bound,
including the nature and purpose of the processing;
(2) the type of personal data subject to the processing, and the
duration of the processing;
(3) the requirements imposed by this subsection and subsections
c. and d. of this section; and
(4) the following requirements:
(a) At the discretion of the controller, the processor shall delete
or return all personal data to the controller as requested at the end of
the provision of services, unless retention of the personal data is
required by law;

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

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

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

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

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

b. Until the first day of the 18th month next following the
effective date of P.L. ___ , c. (C. ___ ) (pending before the
Legislature as this bill), prior to bringing an enforcement action
before an administrative law judge or a court of competent
jurisdiction in this State, the Division of Consumer Affairs in the
Department of Law and Public Safety shall issue a notice to the
controller if a cure is deemed possible. If the operator controller
fails to cure the alleged violation of P.L. ___ , c. (C. ___ ) (pending
before the Legislature as this bill) within 30 days after receiving
notice of alleged noncompliance from the division, such
enforcement action may be brought.\textsuperscript{5}

\textsuperscript{5}15. The Director of the Division of Consumer Affairs in the
Department of Law and Public Safety shall promulgate rules and
regulations, pursuant to the “Administrative Procedure Act,”
P.L.1968, c.410 (C.52:14B-1 et seq.), necessary to effectuate the
purposes of P.L. . , c. (C. ) (pending before the Legislature as
this bill).\textsuperscript{5}

\textsuperscript{5}16. The Office of the Attorney General shall have sole and
exclusive authority to enforce a violation of P.L. . , c. (C. )
(pending before the Legislature as this bill). Nothing in
P.L. . , c. (C. ) (pending before the Legislature as this bill)
shall be construed as providing the basis for, or subject to, a private
right of action for violations of P.L. . , c. (C. ) (pending before
the Legislature as this bill) or under any other law.\textsuperscript{6} \textsuperscript{5}

\textsuperscript{5}17. This act shall take effect on the 365th day following the date
of enactment, except that the Director of the Division of Consumer
Affairs may take any anticipatory administrative action in advance as
shall be necessary for the implementation of this act.\textsuperscript{5}