§§2,4,3,5,6
C.56:8-166.20
to 56:8-166.24
§§7,8
Note

P.L. 2026, CHAPTER 25, ***approved June 30, 2026***
Assembly, No. 5328 ***(First Reprint)***

AN ACT concerning personal data, data brokers, data collectors, and amending P.L.2023, c.266 and supplementing Title 56 of the Revised Statutes.

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

1. Section 9 of P.L.2023, c.266 (C.56:8-166.12) is amended to read as follows:

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.2023, c.266 (C.56:8-166.4 et seq.), 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) <u>not sell sensitive data, which shall apply to all individuals or legal entities regardless of the number of consumers whose data the individual or entity controls or processes;</u>

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 <u>thus</u> is new matter.
Matter enclosed in superscript numerals has been adopted as follows:
[1]Senate floor amendments adopted June 30, 2026.

<u>(7)</u> 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)⟧ <u>(8)</u> 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)⟧ <u>(9)</u> specify the express purposes for which personal data are processed; and

⟦(9)⟧ <u>(10)</u> 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.2023, c.266 (C.56:8-166.4 et seq.) 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.

(cf: P.L.2023, c.266, s.9)

2. (New section) a. As used in P.L. , c. (C.) (pending before the Legislature as this bill):

"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.

"Data broker" means a person or legal entity, including, but not limited to, a controller, that knowingly collects or purchases the personal data of a consumer with whom the person or legal entity does not have a direct relationship and sells or licenses that data to a third party. A third party shall not include a processor if licensure or disclosure of personal data to the processor is solely to process the personal data on the data broker's or data controller's behalf. "Data broker" shall not include a government entity, including any federal agency or State agency as defined in section 2 of P.L.1971, c.182 (C.52:13D-13), any political subdivision, or any division, board, bureau, office, commission, or other instrumentality created by a political subdivision. Examples of a direct relationship include if the consumer is a past or present: (1) customer, client, subscriber, or user of the person or legal entity's goods or services; (2) employee, contractor, or agent of the person or legal entity; (3) investor in the person or legal entity; or (4) donor to the person or legal entity.

"Data collector" means a business, or units of a business, separately or together, that knowingly: (1) collect the personal data of a consumer with whom the data collector has a direct relationship; and (2) sell or license such personal data to a data broker. "Data collector" shall not include a government entity, including any federal agency or State agency as defined in section 2 of P.L.1971, c.182 (C.52:13D-13), any political subdivision, or any division, board, bureau, office, commission, or other instrumentality created by a political subdivision.

"De-identified data" means: data that cannot be reasonably used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the data broker or data [1]**[**controller**]** <u>collector</u>[1] 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 and enforces or otherwise ensures compliance with such obligation.

"Director" means the Director of the Division of Consumer Affairs in the Department of Law and Public Safety.

"Division" means the Division of Consumer Affairs in the Department of Law and Public Safety.

"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" shall 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 [1]**[**controller**]** data broker or data collector[1] directing a processor to process personal data.

"Processor" means a person, private entity, public entity, agency, or other entity that solely processes personal data on behalf of the [1]**[**controller**]** data broker or data collector[1].

"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 [1]**[**controller**]** data broker or data collector[1] 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" or "sell" means sharing, disclosing, or transferring personal data for monetary or other valuable consideration.

"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.

b. The Division of Consumer Affairs in the Department of Law and Public Safety shall establish and maintain a public registry of data brokers and data collectors engaged in [1]**[**processing**]** <u>selling or licensing</u>[1] personal data of New Jersey consumers. Using the information submitted pursuant to subsection c. of this section, the registry shall include, at a minimum, for each data broker and data collector: the data broker's or data collector's name and physical address; a general email address that may be used to request information about the data broker's or data collector's privacy policies and data collection practices; a general Internet website address for the data broker or data collector; an Internet website address specific to the data broker's or data collector's privacy policies; and any relevant opt-out information. The division shall review and update the information contained in the registry at least annually. The division shall not publish any information that is submitted to the division pursuant to paragraph (6) of subsection d. of this section.

c. (1) Each data broker and data collector engaged in selling or licensing personal data of New Jersey consumers shall annually register with the division and pay to the division a registration fee in accordance with paragraph (2) of this subsection. Registration fees collected pursuant to this subsection shall be used as necessary to effectuate the purposes of this act.

(2) The registration fee schedule shall be as follows for a data broker that [1]**[**possesses**]** <u>sells or licenses</u>[1], or a data collector that collects and sells or licenses to a data broker, the personal data of:

(a) 100,000 consumers or fewer in the State—$5,000;

(b) more than 100,000 and fewer than 500,000 consumers in the State—$10,000;

(c) more than 500,000 and fewer than one million consumers in the State—$100,000;

(d) more than one million and fewer than 1.5 million consumers in the State—$500,000;

(e) more than 1.5 million and fewer than 2.5 million consumers in the State—$750,000;

(f) more than 2.5 million and fewer than 4.5 million consumers in the State—$1,000,000; and

(g) more than 4.5 million consumers in the State—$1,500,000.

d. Each data broker and each data collector shall submit the following information to the division at the time of registration, which information shall be updated by the data broker or data collector at least annually, or at such other frequency as the division may require:

(1) the data broker's or data collector's name and primary physical, email, and Internet website addresses;

(2) whether the data broker or data collector permits individuals to opt out of the data broker's or data collector's collection practices, including the method for requesting an opt-out, the type

of opt-out, whether the opt-out is limited to certain activities or sales, and whether the data broker or data collector permits individuals to authorize a third party to opt out on the individual's behalf;

(3) whether the data broker or data collector permits individuals to direct the data broker or data collector to delete any personal data in the data broker's or data collector's possession;

(4) a statement specifying the data collection, databases, or sales activities from which an individual may not opt out;

(5) whether the data broker or data collector uses a credentialing process for purchasers of data and, if applicable, a general explanation of that process;

(6) a history of data breaches and other cybersecurity events affecting the data broker or data collector and personal [1]⟦identifying information⟧ data[1] in the data broker's or data collector's possession, including the number of individuals affected by each data breach or cybersecurity event;

(7) a separate statement detailing the data collection practices, databases, sales activities, and opt-out methods that are applicable to the personal [1]⟦identifying information⟧ data[1] of persons under the age of 18 and whether the data broker or data collector has actual knowledge that it possesses the personal [1]⟦identifying information⟧ data[1] of persons under the age of 18;

(8) any information the division deems appropriate to implement the purposes of P.L.   , c.   (C.   ) (pending before the Legislature as this bill) as identified in regulations adopted pursuant to the "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et seq.); and

(9) the processors who process personal data on behalf of the data broker or data [1]⟦controller⟧ collector[1].

e. A person or entity that knowingly collects or purchases the personal data of a consumer with whom the person or legal entity does not have a direct relationship and sells or licenses data to third parties shall not be considered a data broker or data collector for the purposes of this section if:

(1) the full extent to which the person or entity collects or purchases the personal data of a consumer with whom the person or legal entity does not have a direct relationship and sells, licenses or otherwise provides that data to third parties is incidental to conducting one or more of the following activities:

(a) developing or maintaining a third-party e-commerce or application platform;

(b) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(c) providing publicly available information related to an individual's business or profession or related to providing financial or real estate services;

(d) providing publicly available information via real-time or near real-time alert services for health or safety purposes; or

(e) providing title and settlement services that are regulated and examined by the New Jersey Department of Banking and Insurance; or

(2) the person or entity is a nonprofit organization established to provide enrollment data reporting services on behalf of postsecondary educational institutions.

f. A person or entity that engages in one or more of the activities described in subparagraphs (a) through (d) of paragraph (1) of subsection e. of this section shall be considered a data broker or data collector for the purposes of P.L. , c. (C.) (pending before the Legislature as this bill) if the person or entity collects and or purchases the personal data of a consumer with whom the person or legal entity does not have a direct relationship and sells or licenses data to third parties in any way that is not incidental to an activity described in subparagraphs (a) through (d) of paragraph (1) of subsection e. of this section, unless the person or entity is exempt under paragraph (2) of subsection e. of this section.

g. Nothing in this section shall apply to:

(1) 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" ("HIPAA"), Pub.L.104-191, and the "Health Information Technology for Economic and Clinical Health Act," 42 U.S.C. s.17921 et seq.; or information treated like protected health information collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is used or disclosed in accordance with HIPAA and the information is afforded all the privacy protections and security safeguards of the federal laws and implementing regulations under HIPAA;

(2) 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;

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

(5) the sale of a consumer's personal data by the New Jersey Motor Vehicle Commission that is permitted by the federal "Driver's Privacy Protection Act of 1994," 18 U.S.C. s.2721 et seq.;

(6) 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;

(7) 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;

(8) 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; human subjects research conducted in accordance with good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; or research conducted in accordance with the protection of human subjects pursuant to 21 C.F.R. Parts 50 and 56;

(9) an insurance-support organization as defined in section 2 of P.L.1985, c.179 (C.17:23A-2); or

(10) the person or entity is a national securities association registered pursuant to section 15A of the "Securities Exchange Act of 1934," 15 U.S.C. s.78a et seq., and any rules or regulations promulgated thereunder.

3. (New section) a. In no case shall a data broker or data collector sell or license sensitive data to any other individual or entity.

b. For the purposes of this section only, nothing in this section shall apply to:

(1) 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" ("HIPAA"), Pub.L.104-191, and the "Health Information Technology for Economic and Clinical Health Act," 42 U.S.C. s.17921 et seq.; or information treated like protected health information collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is used or disclosed in accordance with HIPAA and the information is afforded all the privacy protections and security safeguards of the federal laws and implementing regulations under HIPAA;

(2) 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;

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

(5) the sale of a consumer's [1][personal] sensitive[1] data by the New Jersey Motor Vehicle Commission that is permitted by the federal "Driver’s Privacy Protection Act of 1994," 18 U.S.C. s.2721 et seq.;

(6) [1][personal] sensitive[1] 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 [1][personal] sensitive[1] 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;

(7) 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;

(8) [1][personal] sensitive[1] 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; human subjects research conducted in accordance with good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; or research conducted in accordance with the protection of human subjects pursuant to 21 C.F.R. Parts 50 and 56;

(9) an insurance-support organization as defined in section 2 of P.L.1985, c.179 (C.17:23A-2); or

(10) a national securities association registered pursuant to section 15A of the “Securities Exchange Act of 1934,” 15 U.S.C. s.78a et seq., and any rules or regulations promulgated thereunder.

4. (New section) a. A data broker or data collector that fails to register with the division or to submit the annual registration fee as required under subsection c. of section 2 of P.L. , c. (C.) (pending before the Legislature as this bill) shall be liable for, in addition to such registration fees for each year the data broker or data collector failed to register with the division, a civil penalty of $2,500 for each day the data broker or data collector fails to register or submit the required fee.

b. A data broker or data collector that fails to submit or update the information required under subsection d. of section 2 of P.L. , c. (C.) (pending before the Legislature as this bill) shall be liable for a civil penalty of $2,500 for each day the data broker or data collector fails to submit or update the information.

c. A civil penalty assessed pursuant to this section, in addition to any other penalties imposed by law, shall be collected and enforced by the division in a summary proceeding before a court of competent jurisdiction pursuant to the provisions of the "Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.).

5. (New section) A data broker [1], including a controller,[1] or data collector, [1]**[**including a controller,**]**[1] that sells, offers for sale, or licenses sensitive data in violation of paragraph (6) of subsection a. of section 9 of P.L.2023, c.266 (C.56:8-166.12) or section 3 of P.L. , c. (C.) (pending before the Legislature as this bill) shall be liable to a civil penalty of $50,000 for each record sold, offered for sale, or licensed.

6. (New section) The provisions of this act shall be construed as applying in addition to and not in lieu of the provisions of P.L.2023, c.266 (C.56:8-166.4 et seq.).

7. (New section) The Director of the Division of Consumer Affairs in the Department of Law and Public Safety shall adopt rules and regulations, pursuant to the "Administrative Procedure Act," P.L.1968, c.410 (C.52:14B-1 et seq.), as shall be necessary for the implementation of P.L. , c. (C.) (pending before the Legislature as this bill).

8. This act shall take effect immediately, except that [1]subsection b. of[1] section 2 of this act shall remain inoperative for 270 days following the date of enactment.

Regulates data brokers, data collectors, and collection and dissemination of certain sensitive information.