

# SENATE, No. 269

## STATE OF NEW JERSEY 219th LEGISLATURE

PRE-FILED FOR INTRODUCTION IN THE 2020 SESSION

**Sponsored by:**

**Senator THOMAS H. KEAN, JR.**

**District 21 (Morris, Somerset and Union)**

**SYNOPSIS**

Requires certain businesses to notify data subjects of collection of personally identifiable information and establishes certain security standards.

**CURRENT VERSION OF TEXT**

Introduced Pending Technical Review by Legislative Counsel.



1 AN ACT concerning certain businesses and personally identifiable  
2 information 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 “Biometric data” means an individual’s physiological, biological,  
10 or behavioral characteristics, such as an individual’s  
11 deoxyribonucleic acid (DNA), fingerprint, voice print, retina or iris  
12 image or other unique physical representation, that can be used,  
13 singly or in combination with each other or with other identifying  
14 data, to establish an individual’s identity.

15 “Business” means a corporation, partnership, firm, enterprise,  
16 franchise, association, trust, sole proprietorship, union, political  
17 organization, or other legal entity other than a State agency or any  
18 political subdivision thereof, federal agency, or any contractor or  
19 subcontractor employed by a State agency, political subdivision  
20 thereof, or federal agency, that does business in this State and that  
21 shall:

22 have an annual gross revenue of \$5,000,000 or more;  
23 derive 50 percent or more of its annual revenue from selling the  
24 personally identifiable information of data subjects; or  
25 alone or in combination, annually buys, receives, sells, or shares  
26 for commercial purposes the personally identifiable information of  
27 at least 25,000 data subjects.

28 “Data subject” means an individual within this State who  
29 provides, either knowingly or unknowingly, personally identifiable  
30 information to a business.

31 “Deidentified information” means information that cannot  
32 reasonably identify, relate to, describe, be capable or being  
33 associated with, or be linked, directly or indirectly, to a particular  
34 data subject, provided that a business that uses deidentified  
35 information has:

36 implemented technical safeguards that prohibit reidentification  
37 of the data subject to whom the information pertains;

38 implemented business processes that specifically prohibit  
39 reidentification of the information;

40 implemented business process to prevent inadvertent release of  
41 deidentified information; and

42 made no attempt to reidentify the information.

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

1       “Encryption” means the use of an algorithmic process to  
2 transform data into a form in which there is a low probability of  
3 assigning meaning without the use of a confidential process or key.

4       “Information system” means a discrete set of electronic  
5 information resources organized for the collection, processing,  
6 maintenance, use, sharing, dissemination, or disposition of  
7 electronic information, as well as any specialized system, such as  
8 industrial process control systems, telephone switching and private  
9 branch exchanges, and environmental control systems.

10       “Owns or licenses” means receiving, storing, maintaining,  
11 processing, disclosing, or otherwise having access to a data  
12 subject’s personally identifiable information in connection with the  
13 provision of goods or services or in connection with employment.

14       “Personally identifiable information” means any information that  
15 personally identifies, describes, or is able to be associated with a  
16 data subject, including, but not limited to:

- 17       name, alias, nickname, and user name;
- 18       postal and electronic mail address;
- 19       telephone number;
- 20       account name;
- 21       social security number or other government-issued identification  
22 number, including driver’s license number or passport number;
- 23       birthdate or age;
- 24       physical characteristic information, including height and weight;
- 25       biometric data;
- 26       sexual information, including sexual orientation, sex, gender  
27 status, gender identity, and gender expression;
- 28       race or ethnicity;
- 29       religious affiliation or activity;
- 30       political affiliation or activity;
- 31       professional or employment-related information;
- 32       educational information;
- 33       medical information, including, but not limited to, medical  
34 conditions or drugs, therapies, mental health, or medical products or  
35 equipment used;
- 36       financial information, including, but not limited to, credit, debit,  
37 or account numbers, account balances, payment history, or  
38 information related to assets, liabilities, or general creditworthiness;
- 39       commercial information, including, but not limited to, records of  
40 property, products, or services provided, obtained or considered, or  
41 other purchasing or consumer histories;
- 42       geolocation information;
- 43       Internet or mobile activity information, including, but not limited  
44 to, Internet Protocol addresses or information concerning the access  
45 or use of any online service;
- 46       content, including, but not limited to, text, photographs, audio or  
47 video recordings, or other material generated by or provided by the  
48 data subject; and

1 any of the above categories of information as they pertain to the  
2 children of the data subject.

3 “Processing” means the collection, access to, disclosure of, or  
4 storage of personally identifiable information.

5 “Security incident” means any act that results in the unauthorized  
6 access to a data subject’s personally identifiable information or the  
7 disruption or misuse of an information system or information stored  
8 on an information system.

9 “Third party” means:

10 a private entity that is a separate legal entity from the business;

11 a private entity that does not share common ownership or  
12 common corporate control with the business; or

13 a private entity that does not share a brand name or common  
14 branding with the business, such as an affiliate relationship that is  
15 clear to the customer.

16 “Third party service provider” means any person that receives,  
17 stores, maintains, processes, or otherwise is permitted to access a  
18 data subject’s personally identifiable information through the  
19 provision of a service directly to a business.

20

21 2. a. A business that collects a data subject’s personally  
22 identifiable information shall, at or before the point of collection,  
23 state the following:

24 (1) a complete description of the personally identifiable  
25 information that the business collects about a data subject and the  
26 means by which a business collects the personally identifiable  
27 information;

28 (2) the purpose and legal basis for the processing of the  
29 personally identifiable information;

30 (3) all third parties with which the business may disclose a data  
31 subject’s personally identifiable information;

32 (4) the purpose of the disclosure of personally identifiable  
33 information, including whether the business profits from the  
34 disclosure; and

35 (5) the contact information of the person employed at the  
36 business responsible for personally identifiable information data  
37 protection, where applicable.

38 b. The business, at the time the personally identifiable  
39 information is obtained, shall provide the data subject with the  
40 following information for the purpose of ensuring fair and  
41 transparent processing:

42 (1) the period for which the personally identifiable information  
43 will be stored or the criteria used to determine that period; and

44 (2) the right of the data subject to request from the business  
45 access to their personally identifiable information, pursuant to  
46 section 3 of P.L. , c. (C. ) (pending before the Legislature as  
47 this bill).

1 c. The information required to be provided to a data subject  
2 pursuant to subsections a. and b. of this section shall be provided in  
3 a concise, transparent, intelligible, and easy accessible form, using  
4 clear and plain language and shall be provided in writing or by  
5 other means, including electronically.

6  
7 3. a. A business that collects a data subject's personally  
8 identifiable information shall make the following information  
9 available to the data subject free of charge upon receipt of a request  
10 from the data subject for this information through a designated  
11 request address:

12 (1) confirmation that the data subject's personally identifiable  
13 information is, or has been, processed; and

14 (2) a copy of the data subject's personally identifiable  
15 information that has been processed that the data subject can access  
16 in a structured and commonly-used machine-readable format.

17 b. A business that receives a request from a data subject  
18 pursuant to this section shall provide a response to the data subject  
19 within 30 calendar days of the business's receipt of the request and  
20 shall deliver the requested information by mail or in electronic  
21 format.

22 c. A business shall provide information pursuant to this section  
23 at any time but shall not be required to provide this information to a  
24 data subject more than twice annually.

25 d. A business shall correct without unreasonable delay any  
26 inaccurate personally identifiable information at the data subject's  
27 direction.

28 e. The provisions of this section shall not apply to personally  
29 identifiable information disclosed by a business prior to the  
30 effective date of P.L. , c. (C. ) (pending before the  
31 Legislature as this bill).

32  
33 4. A business shall allow a data subject to opt out, in a  
34 reasonable form and manner as determined by the business, at any  
35 time during processing of the data subject's personally identifiable  
36 information, and upon receipt of the data subject's opt out  
37 notification, shall cease processing the data subject's personally  
38 identifiable information unless the processing of a data subject's  
39 personally identifiable information between a business and a third  
40 party is:

41 a. under a written contract authorizing the third party to use the  
42 personally identifiable information to perform services on behalf of  
43 the business, including maintaining or servicing accounts, providing  
44 customer service, processing or fulfilling orders and transactions,  
45 verifying the data subject's information, processing payments,  
46 providing financing, or similar services, but only if the contract  
47 prohibits the third party from using the personally identifiable  
48 information for any reason other than performing the specified

1 service on behalf of the business and from disclosing personally  
2 identifiable information to additional third parties;

3 b. based on a good-faith belief that the processing is required to  
4 comply with any applicable law, rule, or regulation, legal process,  
5 or court order; or

6 c. reasonably necessary to address fraud, security, or technical  
7 issues, to protect the business's rights or property, or to protect a  
8 data subject or the public from illegal activities as required by law.

9

10 5. A business shall maintain an information security program  
11 that meets the requirements for any information security program  
12 required by federal law or, if applicable, that meets industry  
13 standards.

14

15 6. The requirements imposed on a business pursuant to P.L. ,  
16 c. (C. ) (pending before the Legislature as this bill) shall not  
17 restrict a business's ability to:

18 a. comply with federal, State, or local law;

19 b. comply with a civil, criminal, or regulatory inquiry,  
20 investigation, subpoena, or summons by federal, State, or local  
21 authorities;

22 c. cooperate with law enforcement agencies concerning the  
23 conduct of a third party service provider or a third party the  
24 business reasonably believes may violate federal, State, or local  
25 law;

26 d. exercise or defend legal claims; or

27 e. collect, use, retain, sell, or disclose a data subject's  
28 personally identifiable information that has been deidentified or in  
29 aggregate data subject information.

30

31 7. a. In addition to any penalties that may apply pursuant to  
32 the "Identity Theft Protection Act," P.L.2005, c.226 (C.56:11-44 et  
33 al.), it shall be an unlawful practice and violation of P.L.1960, c.39  
34 (C.56:8-1 et seq.) for a business to fail to comply with any of the  
35 provisions of P.L. , c. (C. ) (pending before the Legislature  
36 as this bill) that results in the unauthorized access and exfiltration,  
37 theft, or disclosure of a data subject's personally identifiable  
38 information.

39 b. A business shall be liable, after a 30 day notice to cure that  
40 may include complementary dispute resolution pursuant to Rule  
41 1:40 of the Rules Governing the Courts of the State of New Jersey,  
42 to an affected data subject for any violation pursuant to subsection  
43 a. of this section for a civil penalty of not less than \$100 and not  
44 more than \$750 per data subject per security incident, or actual  
45 damages, whichever is greater, and may be recoverable by the data  
46 subject in a civil action in a court of competent jurisdiction, which  
47 may also order injunctive relief or any other relief the court deems  
48 necessary.

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

7  
8 9. This act shall take effect immediately but shall remain  
9 inoperative until January 1, 2020.

10

11

12

STATEMENT

13

14 This bill requires certain businesses to disclose to people who  
15 knowingly or unknowingly reveal personally identifiable  
16 information to that business that the business is collecting that  
17 information and that the person may opt out of the collection.  
18 Further, this bill sets forth certain security requirements for  
19 businesses that collect the personally identifiable information of a  
20 person, or data subject. “Business,” “data subject,” and “personally  
21 identifiable information” are defined in the bill.

22 A business that collects a data subject’s personally identifiable  
23 information is to, at or before the point of collection, state the  
24 following:

25 (1) a complete description of the personally identifiable  
26 information that the business collects about a data subject and the  
27 means by which a business collects the personally identifiable  
28 information;

29 (2) the purpose and legal basis for the processing of the  
30 personally identifiable information;

31 (3) all third parties with which the business may disclose a data  
32 subject’s personally identifiable information;

33 (4) the purpose of the disclosure of personally identifiable  
34 information, including whether the business profits from the  
35 disclosure and

36 (5) the contact information of the person employed at the  
37 business responsible for personally identifiable information data  
38 protection, where applicable.

39 The bill further provides that the business, at the time the  
40 personally identifiable information is obtained, is to provide the  
41 data subject with the following information for the purpose of  
42 ensuring fair and transparent processing:

43 (1) the period for which the personally identifiable information  
44 will be stored or the criteria used to determine that period; and

45 (2) the right of the data subject to request from the business  
46 access to their personally identifiable information.

47 The information required to be provided is to be provided in a  
48 concise, transparent, intelligible, and easy accessible form, using

1 clear and plain language and is to be provided in writing or by other  
2 means, including electronically.

3 This bill requires a business that collects a data subject's  
4 personally identifiable information to make the following  
5 information available to the data subject free of charge upon receipt  
6 of a request from the data subject for this information through a  
7 toll-free telephone number or email address:

8 (1) confirmation that the data subject's personally identifiable  
9 information is, or has been, processed; and

10 (2) a copy of the data subject's personally identifiable  
11 information that has been processed that the data subject can access  
12 in a structured and commonly-used machine-readable format.

13 A business that receives a request from a data subject is to  
14 provide a response to the data subject within 30 days of the  
15 business's receipt of the request and is to deliver the requested  
16 information by mail or in electronic format. A business is to provide  
17 this information at any time but is not to be required to provide this  
18 information to a data subject more than twice annually. Further, this  
19 bill provides that a business is to correct without unreasonable delay  
20 any inaccurate personally identifiable information at the data  
21 subject's direction.

22 This bill provides that a business is to allow a data subject to opt  
23 out, in a reasonable form and manner as determined by the business,  
24 at any time during processing of the data subject's personally  
25 identifiable information, and upon receipt of the data subject's opt  
26 out notification, is to cease processing the data subject's personally  
27 identifiable information unless the processing of a data subject's  
28 personally identifiable information between a business and a third  
29 party is:

30 (1) under a written contract authorizing the third party to use the  
31 personally identifiable information to perform services on behalf of  
32 the business, including maintaining or servicing accounts, providing  
33 customer service, processing or fulfilling orders and transactions,  
34 verifying the data subject's information, processing payments,  
35 providing financing, or similar services, but only if the contract  
36 prohibits the third party from using the personally identifiable  
37 information for any reason other than performing the specified  
38 service on behalf of the business and from disclosing personally  
39 identifiable information to additional third parties;

40 (2) based on a good-faith belief that the processing is required to  
41 comply with any applicable law, rule, or regulation, legal process,  
42 or court order; or

43 (3) reasonably necessary to address fraud, security, or technical  
44 issues, to protect the business's rights or property, or to protect a  
45 data subject or the public from illegal activities as required by law.

46 The requirements imposed on a business by this bill are not to  
47 restrict a business's ability to:

48 (1) comply with federal, State, or local law;

- 1 (2) comply with a civil, criminal, or regulatory inquiry,  
2 investigation, subpoena, or summons by federal, State, or local  
3 authorities;
- 4 (3) cooperate with law enforcement agencies concerning the  
5 conduct of a third party service provider or a third party the  
6 business reasonably believes may violate federal, State, or local  
7 law;
- 8 (4) exercise or defend legal claims; or
- 9 (5) collect, use, retain, sell, or disclose a data subject's  
10 personally identifiable information that has been deidentified or in  
11 aggregate data subject information.
- 12 The bill provides that it is to be an unlawful practice and  
13 violation of State law for a business to fail to comply with any of  
14 the provisions of this bill that results in the unauthorized access and  
15 exfiltration, theft, or disclosure of a data subject's personally  
16 identifiable information. A business is to be liable to an affected  
17 data subject for any violation for a civil penalty of not less than  
18 \$100 and not more than \$750 per data subject per security incident,  
19 or actual damages, whichever is greater, and may be recoverable by  
20 the data subject in a civil action in a court of competent jurisdiction,  
21 which may also order injunctive relief or any other relief the court  
22 deems necessary.