ASSEMBLY, No. 4640

STATE OF NEW JERSEY

218th LEGISLATURE

INTRODUCED OCTOBER 22, 2018

Sponsored by:
Assemblywoman VALERIE VAINIERI HUTTLE
District 37 (Bergen)
Assemblyman JAMEL C. HOLLEY
District 20 (Union)

SYNOPSIS

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

CURRENT VERSION OF TEXT

As introduced.

(Sponsorship Updated As Of: 10/23/2018)

AN ACT concerning certain businesses 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):

"Biometric data" means an individual's physiological, biological, or behavioral characteristics, such as an individual's deoxyribonucleic acid (DNA), fingerprint, voice print, retina or iris image or other unique physical representation, that can be used, singly or in combination with each other or with other identifying data, to establish an individual's identity.

"Business" means a corporation, partnership, firm, enterprise, franchise, association, trust, sole proprietorship, union, political organization, or other legal entity other than a State agency or any political subdivision thereof, federal agency, or any contractor or subcontractor employed by a State agency, political subdivision thereof, or federal agency, that does business in this State and that shall:

have an annual gross revenue of $5,000,000 or more;

derive 50 percent or more of its annual revenue from selling the personally identifiable information of data subjects; or

alone or in combination, annually buys, receives, sells, or shares for commercial purposes the personally identifiable information of at least 25,000 data subjects.

"Data subject" means an individual within this State who provides, either knowingly or unknowingly, personally identifiable information to a business.

"Deidentified information" means information that cannot reasonably identify, relate to, describe, be capable or being associated with, or be linked, directly or indirectly, to a particular data subject, provided that a business that uses deidentified information has:

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

implemented business processes that specifically prohibit reidentification of the information;

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

made no attempt to reidentify the information.

"Designated request address" means an electronic mail address or toll-free telephone number that a data subject 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).

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

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

"Owns or licenses" means receiving, storing, maintaining, processing, disclosing, or otherwise having access to a data subject's personally identifiable information in connection with the provision of goods or services or in connection with employment.

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

name, alias, nickname, and user name;

postal and electronic mail address;

telephone number;

account name;

social security number or other government-issued identification number, including driver's license number or passport number;

birthdate or age;

physical characteristic information, including height and weight;

biometric data;

sexual information, including sexual orientation, sex, gender status, gender identity, and gender expression;

race or ethnicity;

religious affiliation or activity;

political affiliation or activity;

professional or employment-related information;

educational information;

medical information, including, but not limited to, medical conditions or drugs, therapies, mental health, or medical products or equipment used;

financial information, including, but not limited to, credit, debit, or account numbers, account balances, payment history, or information related to assets, liabilities, or general creditworthiness;

commercial information, including, but not limited to, records of property, products, or services provided, obtained or considered, or other purchasing or consumer histories;

geolocation information;

Internet or mobile activity information, including, but not limited to, Internet Protocol addresses or information concerning the access or use of any online service;

content, including, but not limited to, text, photographs, audio or video recordings, or other material generated by or provided by the data subject; and

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

"Processing" means the collection, access to, disclosure of, or storage of personally identifiable information.

"Security incident" means any act that results in the unauthorized access to a data subject's personally identifiable information or the disruption or misuse of an information system or information stored on an information system.

"Third party" means:

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

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

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

"Third party service provider" means any person that receives, stores, maintains, processes, or otherwise is permitted to access a data subject's personally identifiable information through the provision of a service directly to a business.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. under a written contract authorizing the third party to use the personally identifiable information to perform services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying the data subject's 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 business and from disclosing personally identifiable information to additional third parties;

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

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

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

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

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

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

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

d. exercise or defend legal claims; or

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

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

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

8. 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).

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

STATEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) under a written contract authorizing the third party to use the personally identifiable information to perform services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying the data subject's 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 business and from disclosing personally identifiable information to additional third parties;

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

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

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

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

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, State, or local authorities;

(3) cooperate with law enforcement agencies concerning the conduct of a third party service provider or a third party the business reasonably believes may violate federal, State, or local law;

(4) exercise or defend legal claims; or

(5) collect, use, retain, sell, or disclose a data subject's personally identifiable information that has been deidentified or in aggregate data subject information.

The bill provides that it is to be an unlawful practice and violation of State law for a business to fail to comply with any of the provisions of this bill that results in the unauthorized access and exfiltration, theft, or disclosure of a data subject's personally identifiable information. A business is to be liable to an affected data subject for any violation for a civil penalty of not less than $100 and not more than $750 per data subject per security incident, or actual damages, whichever is greater, and may be recoverable by the data subject in a civil action in a court of competent jurisdiction, which may also order injunctive relief or any other relief the court deems necessary.