ASSEMBLY, No. 3283

STATE OF NEW JERSEY

219th LEGISLATURE

INTRODUCED FEBRUARY 25, 2020

Sponsored by:
Assemblyman ANDREW ZWICKER
District 16 (Hunterdon, Mercer, Middlesex and Somerset)
Assemblywoman VALERIE VAINIERI HUTTLE
District 37 (Bergen)

Co-Sponsored by:
Assemblyman Benson

SYNOPSIS

"New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)"; establishes certain requirements for disclosure and processing of personally identifiable information; establishes Office of Data Protection and Responsible Use in Division of Consumer Affairs.

CURRENT VERSION OF TEXT

As introduced.

(Sponsorship Updated As Of: 3/16/2020)

AN ACT concerning the disclosure and processing of 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. This bill shall be known and may be cited as the "New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)."

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

"Automated decision making" means computational process, including one derived from machine learning, statistics, or other data processing, that makes a decision or facilitates human decision making.

"Biometric data" means personally identifiable information concerning the physical, physiological, or behavioral characteristics of a person.

"Consent" means any freely given, specific, informed, and unambiguous indication by a consumer that the consumer gives in a statement or by clear affirmative action, and signifies agreement to the processing of personally identifiable information.

"Consumer" means an individual in this State who provides, either knowingly or unknowingly, personally identifiable information to a controller.

"Controller" means a person or legal entity that collects, maintains, and determines the purposes and means of processing personally identifiable information.

"De-identified information" means: information that cannot be linked to a consumer without additional information that is kept separately; or information 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 25 of P.L. , c. (C.) (pending before the Legislature as this bill), that is subject to a public commitment by the controller 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 a copy of the information required to be provided pursuant to section 5 of P.L. , c. (C.) (pending before the Legislature as this bill).

"Disclose" means to release, transfer, share, disseminate, make available, rent, sell, or otherwise communicate orally, in writing, or by electronic or any other means to a third party or processor a consumer's personally identifiable information.

"Office" means Office of Data Protection and Responsible Use in the Division of Consumer Affairs in the Department of Law and Public Safety established pursuant to section 22 of P.L. , c. (C.) (pending before the Legislature as this bill).

"Person" means a consumer or a minor child in the custody of the consumer.

"Personally identifiable information" means any information that is linked or reasonably linkable to an identified or identifiable consumer, including a minor child in the custody of the consumer. "Personally identifiable information" shall not include de-identified information or publicly available information.

"Portability" means the ability to receive personally identifiable information in a structured, commonly used, and machine-readable format from a controller that shall be able to be transmitted to another controller without formatting hindrance.

"Process" means an operation that is performed on personally identifiable information, whether or not by automated means, including, but not limited to: collection; recording; organization; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission; dissemination or otherwise making available; alignment or combination; restriction; erasure; or destruction.

"Processor" means a person or legal entity that processes information on behalf of a controller.

"Profiling" means any form of automated decision making using personally identifiable information to evaluate certain personal aspects of a person, including, but not limited to, analyzing or predicting aspects concerning that person's performance at work, 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.

"Third party" means an individual, private entity, public entity, agency, or entity other than the consumer, controller, or processor.

"Verified request" means a request that is made by a consumer, a consumer on behalf of a minor child in the custody of a consumer, or a third-party authorized by law to act on behalf of the consumer whose personally identifiable information was processed, and that a controller can reasonably verify as the person whose personally identifiable information was processed, or is a third-party authorized by the consumer to act on the consumer's behalf.

3. a. The collection and processing of a consumer's personally identifiable information shall be:

(1) collected and processed only upon the consumer affirmatively opting in to the collection, pursuant to section 4 of P.L. , c. (C.) (pending before the Legislature as this bill);

(2) processed lawfully, fairly, and in a transparent manner in relation to the consumer;

(3) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(4) adequate, relevant, and limited to what is necessary in relation to the purposes for which the personally identifiable information is processed;

(5) accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personally identifiable information that is inaccurate is erased or rectified without delay;

(6) kept in a form which permits identification of consumers for no longer than is necessary for the purposes for which the personally identifiable information is processed; and

(7) processed in a manner that ensures appropriate security of the personally identifiable information, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

b. A controller shall be responsible for, and be able to demonstrate to the office, established pursuant to section 22 of P.L. , c. (C.) (pending before the Legislature as this bill), in a form and manner determined by the office, compliance with subsection a. of this section.

4. A controller that collects the personally identifiable information of a consumer may lawfully process the personally identifiable information pursuant to P.L. , c. (C.) (pending before the Legislature as this bill) only if at least one of the following applies:

a. the consumer has given affirmative consent to opt in to the processing of the personally identifiable information for at least one specific purpose provided by the controller pursuant to subsection b. of this section;

b. the processing is necessary for the performance of a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

c. the processing is necessary for compliance with a legal obligation to which the controller is subject;

d. the processing is necessary to protect the vital interest of the consumer or another person;

e. the processing is necessary for the performance of a task conducted in the public interest or in the exercise of official authority vested in the controller; or

f. the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the consumer, which require protection of personally identifiable information, including that of a child.

5. a. A controller that collects the personally identifiable information of a consumer shall, at the time when personally identifiable information is collected, provide to a consumer information concerning the processing of that personally identifiable information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in writing, or by other means, including, where appropriate, by electronic means. That provided information shall include, but not be limited to:

(1) the categories of the personally identifiable information that the controller processes;

(2) the categories of all processors and third parties with which the controller may disclose a consumer's personally identifiable information, including processors in other countries or states that may not provide suitable safeguards pursuant to P.L. , c. (C.) (pending before the Legislature as this bill);

(3) the purpose of the processing for which the personally identifiable information is intended and the legal basis for the processing, pursuant to P.L. , c. (C.) (pending before the Legislature as this bill);

(4) a description of the process for a consumer to review and request changes to any of the consumer's personally identifiable information;

(5) 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;

(6) information concerning one or more designated request addresses;

(7) the identity and the contact details of the controller and, where applicable, the controller's representative, designated pursuant to section 14 of P.L. , c. (C.) (pending before the Legislature as this bill);

(8) the period of time for which the personally identifiable information shall be stored, or if that is not possible, the criteria used to determine that period;

(9) notification of the consumer's right to:

(a) request from the controller access to and rectification or erasure of personally identifiable information, restriction of processing concerning the consumer, or to object to processing;

(b) the portability of personally identifiable information;

(c) withdraw consent to processing at any time without affecting the lawfulness of processing based on consent before its withdrawal; and

(d) lodge a complaint with the office, which shall include all contact information for the office;

(10) whether the provision of personally identifiable information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, whether the consumer is obliged to provide the personally identifiable information and, if so, the possible consequences of failure to provide the personally identifiable information;

(11) the existence of automated decision making, including profiling, and meaningful information concerning the logic involved and significance and potential consequences of automated decision making for the consumer; and

(12) any other information the office deems appropriate.

b. Where the controller intends to process a consumer's personally identifiable information for a purpose other than that for which the personally identifiable information was collected, the controller shall provide the consumer prior to that processing with disclosure pursuant to subsection a. of this section for that latest processing.

c. In addition to the requirements of subsection a. of this section, a controller shall include the notification as a section of the controller's privacy policy, which shall not substitute for the requirements of subsection a. of this section.

6. a. The processing of personally identifiable information revealing racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership, and the processing of biometric data for the purpose of uniquely identifying a person, information concerning health or a person's sexual history or orientation shall be prohibited.

b. The provisions of subsection a. of this section shall not apply if:

(1) the consumer has given affirmative consent to opt in to the processing of the personally identifiable information listed in subsection a. of this section for one or more purposes specified by the controller;

(2) the processing is necessary for the purposes of carrying out the obligations and specific rights of the controller or of the consumer pursuant to State or federal law;

(3) the processing is necessary to protect the vital interest of the consumer where the consumer is physically or legally incapable of giving consent;

(4) the processing is conducted in the course of its legitimate activities with appropriate safeguards, as determined by the office,

by a foundation, association, or any other nonprofit entity with a political, philosophical, religious, or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personally identifiable information is not disclosed outside that body without the consumer's consent;

(5) the processing relates to personally identifiable information that is publically available;

(6) the processing is necessary for the establishment, exercise, or defense of legal claims or court order;

(7) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of healthcare pursuant to State or federal law;

(9) the processing is necessary for public health purposes; or

(10) the processing is necessary for archiving purposes in the public, scientific, or historical interest, as determined by the office.

c. The processing of personally identifiable information concerning criminal convictions and offences shall be permitted only under the control of a State or federal agency and with the appropriate safeguards for the rights and freedom of the consumer. A comprehensive register of criminal convictions shall be kept only under the control of a State or federal agency.

7. a. A controller that discloses a consumer's personally identifiable information to a processor or 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 purposes of the processing;

(2) the category or categories of a consumer's personally identifiable information that were disclosed;

(3) the category or categories of the processors and third parties that received the consumer's personally identifiable information;

(4) where possible, the period of time for which the personally identifiable information will be stored by the controller, processor, or third party, or, if not possible, the criteria used to determine that period of time;

(5) if personally identifiable information was not obtained directly from a consumer, any available information concerning the source of that consumer's personally identifiable information;

(6) the existence of automated decision making, including profiling, and information about the logic involved, and the significance and consequences of this processing to the consumer; and

(7) a copy of the personally identifiable information undergoing processing. For more than a single copy, the controller may charge a reasonable fee based on administrative costs.

b. A controller that receives a verified request from a consumer pursuant to subsection a. of this section shall provide a response to the consumer within 30 days of the controller's receipt of the request and shall provide the information pursuant to subsection a. of this section for all disclosures of personally identifiable information.

c. If the controller does not take action on a consumer's verified request the controller shall inform the consumer without undue delay and at the latest within one month of receipt of the verified request of the reasons for not taking action and on the ability for the consumer to lodge a complaint with the office.

d. Where verified requests from a consumer are unfounded, excessive, or repetitive, the controller may either:

(1) charge a reasonable fee taking into account the administrative costs of providing the information or communication; or

(2) refuse to act on the request, following the requirements established pursuant to subsection c. of this section.

e. The controller shall bear the burden of demonstrating the unfounded, excessive, or repetitive character of the request.

f. 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) or to publically available information.

8. a. A consumer shall have the right to obtain by any means from the controller rectification of inaccurate personally identifiable information.

b. A consumer shall have the right to obtain by any means from the controller the erasure of personally identifiable information where one of the following applies:

(1) the personally identifiable information is no longer necessary in relation to the purpose for which it was collected or otherwise processed;

(2) the consumer withdraws consent made pursuant to subsection a. of section 4 of P.L. , c. (C.) (pending before the Legislature as this bill) on which the processing is based and where there is no other legal ground for the processing; or

(3) the consumer objects to the processing pursuant to section 11 of P.L. , c. (C.) (pending before the Legislature as this bill) and there are no overriding legitimate grounds for the processing.

9. a. A consumer shall have the right to obtain by any means from the controller a restriction of processing of personally identifiable information where one of the following applies:

(1) the accuracy of the personally identifiable information is contested by the consumer for a period enabling the controller to verify the accuracy of the personally identifiable information;

(2) the processing is unlawful and the consumer opposes the erasure of the personally identifiable information;

(3) the controller no longer needs the personally identifiable information for the purposes of the processing but the consumer requires that personally identifiable information for the establishment, exercise, or defense of legal claims; or

(4) the consumer has objected to processing pursuant to section 11 of P.L. , c. (C.) (pending before the Legislature as this bill) pending the verification of whether the legitimate grounds of the controller override those of the consumer.

b. Where processing has been restricted pursuant to subsection a. of this section, personally identifiable information, with the exception of storage, shall only be processed with the consumer's consent or for the establishment, exercise, or defense of legal claims or for the protection of the rights of another person or legal entity or for the public interest.

c. A consumer that has obtained restriction pursuant to subsection a. of this section shall be informed by the controller before the restriction of processing is lifted.

10. A controller shall notify each processor and third party to which a controller has disclosed a consumer's personally identifiable information of any rectification or erasure of personally identifiable information made by a consumer pursuant to section 8 of P.L. , c. (C.) (pending before the Legislature as this bill) or restriction of processing made by a consumer pursuant to section 9 of P.L. , c. (C.) (pending before the Legislature as this bill).

11. a. A consumer shall have the right to object, by any means, to the processing of personally identifiable information, at which time the controller shall no longer process the personally identifiable information unless the controller demonstrates compelling legitimate grounds, as determined by the office, for the processing which overrides the interests, rights, and freedoms of the consumer or for the establishment, exercise, or defense of legal claims.

b. Where personally identifiable information is processed for direct marketing purposes, including profiling, the consumer shall have the right to object at any time to processing of personally identifiable information for this purpose, at which time the

personally identifiable information shall no longer be used for this purpose.

c. Where personally identifiable information is processed for scientific or historical research purposes or statistical purposes, the consumer shall have the right to object, by any means, to the processing of their personally identifiable information unless the processing is necessary for the public interest, as determined by the office.

12. a. A consumer shall not be subject to a decision based solely on automated decision making, including profiling, which produces legal effects concerning the consumer or similarly significantly affects the consumer.

b. The provisions of subsection a. of this section shall not apply if the decision:

(1) is necessary for entering into, or performance of, a contract between the consumer and the controller;

(2) is authorized by law and which also includes measures to safeguard the consumer's rights pursuant to section 3 of P.L. , c. (C.) (pending before the Legislature as this bill);

(3) is based on the consumer's explicit consent.

c. The provisions of subsection b. of this section shall not be based on the categories of personally identifiable information listed in section 6 of P.L. , c. (C.) (pending before the Legislature as this bill) unless suitable measures are taken to ensure the consumer's rights, freedoms, and legitimate interests are in place, as determined by the office.

13. a. A controller shall implement the appropriate technical and organizational measures to ensure and to be able to demonstrate to the office that processing is performed in accordance with P.L. , c. (C.) (pending before the Legislature as this bill).

b. Taking into account the technology, cost of implementation, and the nature, scope, context, and purpose of processing, and the rights of the consumer, the controller shall at the time of the determination of the means of processing and at the time of the processing itself, implement technical and organization measures, that are designed to implement data-protection principles and safeguards into the processing in order to meet the requirements of P.L. , c. (C.) (pending before the Legislature as this bill).

c. A controller shall implement technical and organizational measures to ensure that, by default, only personally identifiable information necessary for the specific purpose of processing is processed, including the period of storage.

14. a. A controller and processor shall designate in writing to the office a representative that shall serve as a liaison between the controller or processor and the office and public.

b. The provisions of subsection a. of this section shall not apply to a controller or processor that:

(1) processes personally identifiable information occasionally, does not include, on a large scale, the processing of the categories of personally identifiable information listed in section 6 of P.L. , c. (C.) (pending before the Legislature as this bill), processes criminal convictions and offenses, or processes information in a manner that is unlikely to result in a risk to the rights and freedoms of a person, as determined by the office; or

(2) is a State agency or any political subdivision thereof.

15. a. Where processing is to be conducted on behalf of a controller by a processor, the controller shall contract with a processor providing sufficient guarantees to implement appropriate technical and organization measures in a manner that processing shall meet the requirements of P.L. , c. (C.) (pending before the Legislature as this bill).

b. The processor shall not engage another processor without prior specific or general written authorization of the controller.

c. Processing by a processor shall be governed by a contract between a processor and controller that shall include, but not be limited to:

(1) a stipulation that the processor shall process the personally identifiable information using documented instructions from the controller, including the instructions on the transfer of personally identifiable information to another country or international organization;

(2) a commitment to the confidentiality and data security of the personally identifiable information to be processed required by law;

(3) assistance in cooperating with the controller to fulfill the controller's obligation to respond to consumer requests to exercise rights established pursuant to P.L. , c. (C.) (pending before the Legislature as this bill);

(4) an agreement by the processor to delete or return all personally identifiable information at the request of the controller;

(5) the processor making available to the controller all information necessary to demonstrate compliance with the obligations established pursuant to P.L. , c. (C.) (pending before the Legislature as this bill); and

(6) where the processor engages another processor for carrying out processing on behalf of the controller, that contract shall include the same confidentiality and data security requirements as in the contract between the controller and initial processor.

d. The office may adopt standard contractual clauses for the contracts between a controller and a processor pursuant to the provisions of P.L. , c. (C.) (pending before the Legislature as this bill).

16. a. A controller and, where applicable, the controller's representative, established pursuant to section 14 of P.L. , c. (C.) (pending before the Legislature as this bill), shall maintain a record of processing activities under its responsibility. The record shall contain, but not be limited to, the following information:

(1) the name and contact details of the controller and, where applicable, any other controller, or the controller's representative;

(2) the purpose of the processing;

(3) a description of the categories of consumers and categories of personally identifiable information;

(4) the categories of recipients to whom the personally identifiable information has been or will be disclosed, including recipients in other counties or international organizations;

(5) where possible, the potential time limits for erasure of the different categories of personally identifiable information;

(6) where possible, a description of the technical and organizational security measures required pursuant to section 17 of P.L. , c. (C.) (pending before the Legislature as this bill).

b. A processor and, where applicable, the processor's representative, shall maintain a record of all categories of processing activities carried out on behalf of a controller. The record shall contain, but not be limited to, the following information:

(1) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and, where applicable, of the controller's or the processor's representative;

(2) the categories of processing carried out on behalf of the controller;

(3) where applicable, transfers of personally identifiable information to another country or an international organization;

(4) where possible, a description of the technical and organizational security measures required pursuant to section 17 of P.L. , c. (C.) (pending before the Legislature as this bill).

c. The information required pursuant to subsections a. and b. of this section shall be in writing, including in electronic form, and shall be made available to the office upon request.

17. a. Taking into account the technology, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of a person, the controller and processor shall implement appropriate technical and organization measures to ensure a level of security appropriate to the risk, including, but not limited to:

(1) using de-identified information where possible;

(2) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

(3) the ability to restore the availability and access to personally identifiable information in a timely manner in the event of a physical or technical data breach; and

(4) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organization measures for ensuring the security of the processing.

b. In assessing the appropriate level of security, account shall be taken concerning the risks that are presented by processing, such as from unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personally identifiable information transmitted, stored, or otherwise processed.

c. Adherence to a code of conduct or certification mechanism approved by the office, pursuant to paragraph (1) of subsection b. of section 22 of P.L. , c. (C.) (pending before the Legislature as this bill), may be used as an element by which to demonstrate compliance with the requirements established pursuant to this section.

18. a. Notwithstanding any other law, rule, or regulation to the contrary, in the event of a data breach resulting in the unauthorized access of personally identifiable information, the controller shall immediately and, where feasible, not later than 72 hours after having become aware of it, notify the office. Where the notification to the office is not made within 72 hours, it shall be accompanied by reasons for the undue delay.

b. The processor shall immediately notify the controller after becoming aware of a data breach resulting in the unauthorized access of personally identifiable information and shall contain, but not be limited to, the following information:

(1) a description of the nature of the data breach including the categories and approximate number of consumers affected and the categories and approximate number of compromised records;

(2) the name and contact details where more information can be obtained;

(3) a description of the likely consequences of the data breach; and

(4) a description of the measures taken or proposed to be taken by the processor to address the data breach.

c. The controller shall document any data breaches resulting in the unauthorized access of personally identifiable information, its effects, and remedial action taken, which shall be made available to the office at the office’s request.

19. a. Notwithstanding any other law, rule, or regulation to the contrary, in the event of a data breach resulting in the unauthorized access of personally identifiable information that is likely to result

in a high risk to the rights and freedoms of a person, the controller shall immediately notify a consumer.

b. The data breach notification shall describe in clear and plain language the nature of the data breach and contain, but not be limited to:

(1) the name and contact details where more information can be obtained;

(2) a description of the likely consequences of the data breach; and

(3) a description of the measures taken or proposed to be taken by the controller to address the data breach.

c. Notification pursuant to this section shall not be required if one of the following are met:

(1) the controller has implemented appropriate technical and organization protection measures and those measures were applied to the personally identifiable information affected by the data breach, such as rendering the personally identifiable information unintelligible to any person who is not authorized to access it;

(2) the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of a person are no longer likely to materialize; or

(3) it would involve disproportionate effort, which, in that case, there shall instead be a public communication or similar measure where consumers are informed in an equally effective manner.

d. The office may notify consumers of a data breach resulting in the unauthorized access of personally identifiable information if the office determines there is a high risk to the rights and freedoms of a person.

20. a. A controller shall, prior to processing personally identifiable information, conduct a data protection impact assessment that shall be submitted to the office and that shall contain, but not be limited to:

(1) a systematic description of potential processing operations and the purpose of the processing, including where applicable, the legitimate interest pursued by the controller;

(2) an assessment of the necessity and proportionality of the processing operations in relation to the purpose;

(3) an assessment of the risks to the rights and freedoms of consumers; and

(4) potential measures to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with P.L. , c. (C.) (pending before the Legislature as this bill).

b. The office shall establish and publicize a list of the kind of processing operations that are subject to the requirements of this section.

c. The office may establish and publicize a list of the kind of processing operations for which no data protection impact assessment is required.

d. Where appropriate, a controller shall request input from consumers on the intended processing.

21. a. The controller shall consult with the office prior to processing in the event the data protection impact assessment, required pursuant to section 20 of P.L. , c. (C.) (pending before the Legislature as this bill), indicates that the processing would result in a high risk to a consumer's personally identifiable information in the absence of measures taken by the controller to mitigate the risk.

b. If the office determines that the controller's data protection impact assessment indicates the processing may violate the provisions of P.L. , c. (C.) (pending before the Legislature as this bill), the office shall, within eight weeks of the submission of the data protection impact assessment, provide written advice to the controller, and processor where applicable, concerning best industry practices to conform with the requirements of P.L. , c. (C.) (pending before the Legislature as this bill).

22. a. There is established the Office of Data Protection and Responsible Use in the Division of Consumer Affairs in the Department of Law and Public Safety. The purpose of this office shall be to serve as a clearinghouse of information, comprehensive resource for consumers, controllers, and processors, and regulatory body concerning the security and processing of personally identifiable information.

b. The office's functions shall include, but not be limited to:

(1) direction and oversight to controllers and processors on complying with the provisions of P.L. , c. (C.) (pending before the Legislature as this bill), including developing a code of conduct or certification mechanism for controllers and processors to use in developing data security procedures;

(2) development and distribution of informational materials for consumers concerning personally identifiable information protection best practices, consumer rights concerning personally identifiable information, and any other subject the office deems relevant to fulfilling its functions;

(3) reviewing current and proposed legislation and regulations pertaining to personally identifiable information protection and security and making recommendations concerning potential legislation and regulations;

(4) conducting biannual public hearings for the purpose of gathering public input concerning what types of information constitute personally identifiable information that should be monitored by the office, advancements in technology relating to the

collection of personally identifiable information, and any other subject the office deems relevant to fulfilling its functions;

(5) receiving, cataloging, and investigating reports of potential violations of P.L. , c. (C.) (pending before the Legislature as this bill) and reporting the findings to the Attorney General for potential legal action; and

(6) cooperation with other State and federal agencies with the intent of ensuring the uniform application of P.L. , c. (C.) (pending before the Legislature as this bill).

c. The Attorney General shall, in consultation with the State's Chief Information Officer, appoint an executive director to head the office who shall be an individual qualified by training and experience to perform the duties of the office and who shall devote the time as executive director solely to the performance of those duties.

d. The office shall be entitled to call to its assistance and avail itself of the services of the employees of any State department, board, bureau, commission, or agency it may require and as may be available for its purposes.

23. 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 or an affiliate of a financial institution that is subject to Title V of the federal "Gramm-Leach-Bliley Act of 1999," 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); or

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

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.;

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; and

g. an operator, as that term is defined in section 1 of P.L.2019, c.494 (C.), acting in compliance with the provisions of P.L.2019, c.494 (C.).

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

25. 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).

26. This act shall take effect on the first day of the sixth month following the date of enactment.

STATEMENT

The bill, entitled the "New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)," establishes certain rights for consumers concerning the disclosure and processing of a consumer's personally identifiable information. A controller, as that term is defined in the bill, that collects the personally identifiable information of a consumer may lawfully process the personally identifiable information pursuant certain provisions in the bill only if at least one of the following applies:

1) the consumer has given consent to the processing of the personally identifiable information for at least one specific purpose provided by the controller;

2) processing is necessary for the performance of a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

3) processing is necessary for compliance with a legal obligation to which the controller is subject;

4) processing is necessary to protect the vital interest of the consumer or another person;

5) processing is necessary for the performance of a task conducted in the public interest or in the exercise of official authority vested in the controller; or

6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the consumer, which require protection of personally identifiable information, including that of a child.

The bill provides that a controller that collects the personally identifiable information of a consumer is to, at the time when personally identifiable information is collected, provide to a consumer information concerning the processing of that personally identifiable information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in writing, or by other means, including, where appropriate, by electronic means that shall include, but not be limited to, certain information listed in the bill. The bill further provides that where the controller intends to process a consumer's personally identifiable information for a purpose other than that for which the personally identifiable information was collected, the controller is to provide certain disclosures to the consumer prior to that processing.

The processing of personally identifiable information revealing racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership, and the processing of biometric data for the purpose of uniquely identifying a person, information concerning health or a person's sexual history or orientation is to be prohibited except in certain circumstances provided in the bill.

The bill provides that a controller that discloses a consumer's personally identifiable information to a processor or third party is to make certain information provided in the bill available to the consumer free of charge upon receipt of a verified request from the consumer for this information through a designated request address.

The bill provides that a controller that receives a verified request from a consumer is to provide a response to the consumer within 30 days of the controller's receipt of the request and is to provide information concerning all disclosures of personally identifiable information.

The bill provides that if the controller does not take action on a consumer's verified request the controller is to inform the consumer without undue delay and at the latest within one month of receipt of the verified request of the reasons for not taking action and on the ability for the consumer to lodge a complaint with the Office of Data Protection and Responsible Use (office) in the Division of Consumer Affairs in the Department of Law and Public Safety, established by the bill.

The bill provides that the purpose of the office is to serve as a clearinghouse of information, comprehensive resource for consumers, controllers, and processors, and regulatory body concerning the security and processing of personally identifiable information. The office's functions are enumerated in the bill.

The bill provides that a consumer is to have the right to obtain by any means from the controller rectification of inaccurate personally identifiable information. A consumer is to have the right to obtain by any means from the controller the erasure, or restriction of the processing, of personally identifiable information under certain circumstances provided by the bill.

The bill provides that where processing has been restricted, personally identifiable information, with the exception of storage, is to only be processed with the consumer's consent or for the establishment, exercise, or defense of legal claims or for the protection of the rights of another person or legal entity or for the public interest.

The bill provides that a controller is to notify each processor and third party that received a consumer's personally identifiable information of any rectification or erasure of personally identifiable information made by a consumer pursuant to the bill or restriction of processing made by a consumer pursuant to the bill.

The bill provides that a consumer is to have the right to object, by any means, to the processing of personally identifiable information, at which time the controller is to no longer process the personally identifiable information unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights, and freedoms of the consumer or for the establishment, exercise, or defense of legal claims.

Where personally identifiable information is processed for direct marketing purposes, including profiling, the consumer is to have the right to object at any time to processing of personally identifiable information for this purpose, at which time the personally identifiable information is to no longer be used for this purpose.

The bill provides that where personally identifiable information is processed for scientific or historical research purposes or statistical purposes, the consumer is to have the right to object, by any means, to the processing of their personally identifiable information unless the processing is necessary for the public interest.

The bill provides that a consumer is not to be subject to a decision based solely on automated decision making, including profiling, which produces legal effects concerning the consumer or similarly significantly affects the consumer except under certain circumstances provided in the bill.

The bill provides that a controller is to implement the appropriate technical and organizational measures to ensure and to be able to demonstrate to the office that processing is performed in accordance with the requirements of the bill.

The bill requires a controller and processor, in certain situations provided in the bill, to designate in writing to the office a representative that is to serve as a liaison between the controller or processor and the office and public.

The bill provides that, where processing is to be conducted on behalf of a controller by a processor, the controller is to contract with a processor providing sufficient guarantees to implement appropriate technical and organization measures in a manner that processing shall meet the requirements the bill. The processor shall

not engage another processor without prior specific or general written authorization of the controller.

Processing by a processor is to be governed by a contract between a processor and controller that is to include certain provisions provided in the bill.

The bill allows the office to adopt standard contractual clauses for the contracts between controllers and processors.

The bill provides that a controller and, where applicable, the controller's representative, is to maintain a record of processing activities under its responsibility. A processor and, where applicable, the processor's representative, is to maintain a record of all categories of processing activities carried out on behalf of a controller. These records are to be in writing, including in electronic form, and be made available to the office upon request.

Taking into account the technology, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of a person, the bill requires a controller and processor to implement appropriate technical and organization measures to ensure a level of security appropriate to the risk, including certain measures provided in the bill.

In assessing the appropriate level of security, account is to be taken concerning the risks that are presented by processing, such as from unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personally identifiable information transmitted, stored, or otherwise processed.

Adherence to a code of conduct or certification mechanism approved by the office may be used as an element by which to demonstrate compliance with the requirements established pursuant to the bill.

The bill provides that, notwithstanding any other law, rule, or regulation to the contrary, in the event of a data breach resulting in the unauthorized access of personally identifiable information, the controller is to immediately and, where feasible, not later than 72 hours after having become aware of it, notify the office. Where the notification to the office is not made within 72 hours, it is to be accompanied by reasons for the undue delay.

A processor is to notify the controller immediately after becoming aware of a data breach resulting in the unauthorized access of personally identifiable information and the notice is to contain certain information provided in the bill.

The controller is to document any data breaches resulting in the unauthorized access of personally identifiable information, its effects, and remedial action taken, which is to be made available to the office at the office's request.

The bill further provides that, notwithstanding any other law, rule, or regulation to the contrary, in the event of a data breach resulting in the unauthorized access of personally identifiable

information that is likely to result in a high risk to the rights and freedoms of a person, the controller is to notify a consumer without undue delay.

The bill provides that the data breach notification is to describe in clear and plain language the nature of the data breach but notification is not to be required under certain circumstances provided in the bill.

The bill allows the office to notify consumers of a data breach resulting in the unauthorized access of personally identifiable information if the office determines there is a high risk to the rights and freedoms of a person.

The bill requires a controller to, prior to processing personally identifiable information, conduct a data protection impact assessment that is to contain certain information provided for in the bill.

The office is to establish and publicize a list of the kind of processing operations that are subject to the requirements of the data protection impact assessment. The office may establish and publicize a list of the kind of processing operations for which no data protection impact assessment is required. Where appropriate, a controller is to request input from consumers on the intended processing.

The bill requires a controller to consult with the office prior to processing in the event the data protection impact assessment indicates that the processing would result in a high risk to a consumer's personally identifiable information in the absence of measures taken by the controller to mitigate the risk. If the office determines that the controller's data protection impact assessment indicates the processing may violate the provisions the bill, the office is to, within eight weeks of the submission of the data protection impact assessment, provide written advice to the controller, and processor where applicable, concerning best industry practices to conform with the requirements of the bill.

The Attorney General is to, in consultation with the State's Chief Information Officer, appoint an executive director to head the office who is to be an individual qualified by training and experience to perform the duties of the office and who is to devote the time as executive director solely to the performance of those duties.

It is to be an unlawful practice and violation of the consumer fraud act for a controller or processor to violate any provision of the bill, which includes $10,000 fine for the first offense and a $20,000 for each subsequent offense.