

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)

1 AN ACT concerning the disclosure and processing of personally
2 identifiable information and supplementing Title 56 of the
3 Revised Statutes.

4
5 **BE IT ENACTED** *by the Senate and General Assembly of the State*
6 *of New Jersey:*

7
8 1. This bill shall be known and may be cited as the “New
9 Jersey Disclosure and Accountability Transparency Act (NJ
10 DaTA).”

11
12 2. As used in P.L. , c. (C.) (pending before the
13 Legislature as this bill):

14 “Automated decision making” means computational process,
15 including one derived from machine learning, statistics, or other
16 data processing, that makes a decision or facilitates human decision
17 making.

18 “Biometric data” means personally identifiable information
19 concerning the physical, physiological, or behavioral characteristics
20 of a person.

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

25 “Consumer” means an individual in this State who provides, either
26 knowingly or unknowingly, personally identifiable information to a
27 controller.

28 “Controller” means a person or legal entity that collects,
29 maintains, and determines the purposes and means of processing
30 personally identifiable information.

31 “De-identified information” means: information that cannot be
32 linked to a consumer without additional information that is kept
33 separately; or information that has been modified to a degree that
34 the risk of re-identification, consistent with guidance from the
35 Federal Trade Commission and the National Institute of Standards
36 and Technology, is small, as determined by the Director of the
37 Division of Consumer Affairs in the Department of Law and Public
38 Safety pursuant to section 25 of P.L. , c. (C.) (pending
39 before the Legislature as this bill), that is subject to a public
40 commitment by the controller not to attempt to re-identify the data,
41 and to which one or more enforceable controls to prevent re-
42 identification has been applied, which may include legal,
43 administrative, technical, or contractual controls.

44 “Designated request address” means an electronic mail address,
45 Internet website, or toll-free telephone number that a consumer may
46 use to request a copy of the information required to be provided
47 pursuant to section 5 of P.L. , c. (C.) (pending before the
48 Legislature as this bill).

1 “Disclose” means to release, transfer, share, disseminate, make
2 available, rent, sell, or otherwise communicate orally, in writing, or
3 by electronic or any other means to a third party or processor a
4 consumer’s personally identifiable information.

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

9 “Person” means a consumer or a minor child in the custody of
10 the consumer.

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

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

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

27 “Processor” means a person or legal entity that processes
28 information on behalf of a controller.

29 “Profiling” means any form of automated decision making using
30 personally identifiable information to evaluate certain personal
31 aspects of a person, including, but not limited to, analyzing or
32 predicting aspects concerning that person’s performance at work,
33 economic situation, health, personal preferences, interests,
34 reliability, behavior, location, or movements.

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

38 “Third party” means an individual, private entity, public entity,
39 agency, or entity other than the consumer, controller, or processor.

40 “Verified request” means a request that is made by a consumer, a
41 consumer on behalf of a minor child in the custody of a consumer,
42 or a third-party authorized by law to act on behalf of the consumer
43 whose personally identifiable information was processed, and that a
44 controller can reasonably verify as the person whose personally
45 identifiable information was processed, or is a third-party
46 authorized by the consumer to act on the consumer’s behalf.

- 1 3. a. The collection and processing of a consumer’s personally
2 identifiable information shall be:
- 3 (1) collected and processed only upon the consumer
4 affirmatively opting in to the collection, pursuant to section 4 of
5 P.L. , c. (C.) (pending before the Legislature as this bill);
6 (2) processed lawfully, fairly, and in a transparent manner in
7 relation to the consumer;
- 8 (3) collected for specified, explicit, and legitimate purposes and
9 not further processed in a manner that is incompatible with those
10 purposes;
- 11 (4) adequate, relevant, and limited to what is necessary in
12 relation to the purposes for which the personally identifiable
13 information is processed;
- 14 (5) accurate and, where necessary, kept up to date and every
15 reasonable step shall be taken to ensure that personally identifiable
16 information that is inaccurate is erased or rectified without delay;
- 17 (6) kept in a form which permits identification of consumers for
18 no longer than is necessary for the purposes for which the
19 personally identifiable information is processed; and
- 20 (7) processed in a manner that ensures appropriate security of
21 the personally identifiable information, including protection against
22 unauthorized or unlawful processing and against accidental loss,
23 destruction, or damage, using appropriate technical or
24 organizational measures.
- 25 b. A controller shall be responsible for, and be able to
26 demonstrate to the office, established pursuant to section 22 of
27 P.L. , c. (C.) (pending before the Legislature as this bill), in
28 a form and manner determined by the office, compliance with
29 subsection a. of this section.
- 30
- 31 4. A controller that collects the personally identifiable
32 information of a consumer may lawfully process the personally
33 identifiable information pursuant to P.L. , c. (C.) (pending
34 before the Legislature as this bill) only if at least one of the
35 following applies:
- 36 a. the consumer has given affirmative consent to opt in to the
37 processing of the personally identifiable information for at least one
38 specific purpose provided by the controller pursuant to subsection
39 b. of this section;
- 40 b. the processing is necessary for the performance of a contract
41 to which the consumer is a party or in order to take steps at the
42 request of the consumer prior to entering into a contract;
- 43 c. the processing is necessary for compliance with a legal
44 obligation to which the controller is subject;
- 45 d. the processing is necessary to protect the vital interest of the
46 consumer or another person;

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

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

9
10 5. a. A controller that collects the personally identifiable
11 information of a consumer shall, at the time when personally
12 identifiable information is collected, provide to a consumer
13 information concerning the processing of that personally
14 identifiable information in a concise, transparent, intelligible, and
15 easily accessible form, using clear and plain language, in writing, or
16 by other means, including, where appropriate, by electronic means.
17 That provided information shall include, but not be limited to:

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

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

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

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

32 (5) the process by which the controller notifies consumers of
33 material changes to the notification required to be made available
34 pursuant to this subsection, along with the effective date of the
35 notice;

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

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

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

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

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

1 (b) the portability of personally identifiable information;
2 (c) withdraw consent to processing at any time without affecting
3 the lawfulness of processing based on consent before its
4 withdrawal; and

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

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

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

17 (12) any other information the office deems appropriate.

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

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

28

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

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

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

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

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

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

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

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

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

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

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

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

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

26

27 7. a. A controller that discloses a consumer's personally
28 identifiable information to a processor or third party shall make the
29 following information available to the consumer free of charge
30 upon receipt of a verified request from the consumer for this
31 information through a designated request address:

32 (1) the purposes of the processing;

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

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

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

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

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

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

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

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

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

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

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

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

24 f. This section shall not apply to personally identifiable
25 information disclosed prior to the effective date of P.L. ,
26 c. (C.) (pending before the Legislature as this bill) or to
27 publically available information.

28

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

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

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

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

42 (3) the consumer objects to the processing pursuant to section
43 11 of P.L. , c. (C.) (pending before the Legislature as this
44 bill) and there are no overriding legitimate grounds for the
45 processing.

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

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

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

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

13 (4) the consumer has objected to processing pursuant to section
14 11 of P.L. , c. (C.) (pending before the Legislature as this
15 bill) pending the verification of whether the legitimate grounds of
16 the controller override those of the consumer.

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

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

26

27 10. A controller shall notify each processor and third party to
28 which a controller has disclosed a consumer's personally
29 identifiable information of any rectification or erasure of personally
30 identifiable information made by a consumer pursuant to section 8
31 of P.L. , c. (C.) (pending before the Legislature as this bill)
32 or restriction of processing made by a consumer pursuant to section
33 9 of P.L. , c. (C.) (pending before the Legislature as this
34 bill).

35

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

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

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

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

9
10 12. a. A consumer shall not be subject to a decision based solely
11 on automated decision making, including profiling, which produces
12 legal effects concerning the consumer or similarly significantly
13 affects the consumer.

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

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

18 (2) is authorized by law and which also includes measures to
19 safeguard the consumer's rights pursuant to section 3 of P.L. ,

20 c. (C.) (pending before the Legislature as this bill);

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

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

28
29 13. a. A controller shall implement the appropriate technical
30 and organizational measures to ensure and to be able to demonstrate
31 to the office that processing is performed in accordance with
32 P.L. , c. (C.) (pending before the Legislature as this bill).

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

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

45
46 14. a. A controller and processor shall designate in writing to
47 the office a representative that shall serve as a liaison between the
48 controller or processor and the office and public.

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

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

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

11

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

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

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

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

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

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

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

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

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

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

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

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

9 (2) the purpose of the processing;

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

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

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

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

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

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

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

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

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

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

39
40 17. a. Taking into account the technology, the costs of
41 implementation, and the nature, scope, context, and purposes of
42 processing, as well as the risk of varying likelihood and severity for
43 the rights and freedoms of a person, the controller and processor
44 shall implement appropriate technical and organization measures to
45 ensure a level of security appropriate to the risk, including, but not
46 limited to:

47 (1) using de-identified information where possible;

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

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

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

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

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

20

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

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

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

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

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

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

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

45

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

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

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

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

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

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

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

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

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

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

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

29

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

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

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

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

41 (4) potential measures to address the risks, including safeguards,
42 security measures, and mechanisms to ensure the protection of
43 personal data and to demonstrate compliance with P.L. ,

44 c. (C.) (pending before the Legislature as this bill).

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

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

4 d. Where appropriate, a controller shall request input from
5 consumers on the intended processing.
6

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

14 b. If the office determines that the controller's data protection
15 impact assessment indicates the processing may violate the
16 provisions of P.L. , c. (C.) (pending before the Legislature
17 as this bill), the office shall, within eight weeks of the submission
18 of the data protection impact assessment, provide written advice to
19 the controller, and processor where applicable, concerning best
20 industry practices to conform with the requirements of P.L. ,
21 c. (C.) (pending before the Legislature as this bill).
22

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

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

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

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

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

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

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

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

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

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

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

20

21 23. Nothing in P.L. , c. (C.) (pending before the
22 Legislature as this bill) shall apply to:

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

31 b. a financial institution or an affiliate of a financial institution
32 that is subject to Title V of the federal "Gramm-Leach-Bliley Act of
33 1999," 15 U.S.C. s.6801 et seq., and the rules and implementing
34 regulations promulgated thereunder;

35 c. the secondary market institutions identified in 15 U.S.C.
36 s.6809(3)(D) and 12 C.F.R. s.1016.3(l)(3)(iii); or

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

39 e. the sale of a consumer's personally identifiable information
40 by the New Jersey Motor Vehicle Commission that is permitted by
41 the federal "Drivers' Privacy Protection Act of 1994," 18 U.S.C.
42 s.2721 et seq.;

43 f. personally identifiable information collected, processed,
44 sold, or disclosed by a consumer reporting agency, as defined in 15
45 U.S.C. s.1681a(f), if the collection, processing, sale, or disclosure
46 of the personally identifiable information is limited by the federal
47 "Fair Credit Reporting Act," 15 U.S.C. s.1681 et seq., and
48 implementing regulations; and

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

4
5 24. It shall be an unlawful practice and violation of P.L.1960,
6 c.39 (C.56:8-1 et seq.) for a controller or processor to violate any
7 provision of P.L. , c. (C.) (pending before the Legislature as
8 this bill).

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

16
17 26. This act shall take effect on the first day of the sixth month
18 following the date of enactment.

19
20
21 STATEMENT

22
23 The bill, entitled the “New Jersey Disclosure and Accountability
24 Transparency Act (NJ DaTA),” establishes certain rights for
25 consumers concerning the disclosure and processing of a
26 consumer’s personally identifiable information. A controller, as that
27 term is defined in the bill, that collects the personally identifiable
28 information of a consumer may lawfully process the personally
29 identifiable information pursuant certain provisions in the bill only
30 if at least one of the following applies:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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