



131st MAINE LEGISLATURE

FIRST SPECIAL SESSION-2023

Legislative Document

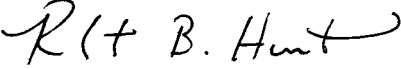
No. 1977

H.P. 1270

House of Representatives, May 22, 2023

An Act to Create the Data Privacy and Protection Act

Reference to the Committee on Innovation, Development, Economic Advancement and Business suggested and ordered printed.


ROBERT B. HUNT
Clerk

Presented by Representative O'NEIL of Saco.
Cosponsored by Senator HICKMAN of Kennebec and
Representatives: BOYER of Poland, BRENNAN of Portland, RIELLY of Westbrook.

1 **Be it enacted by the People of the State of Maine as follows:**

2 **Sec. 1. 10 MRSA c. 1057** is enacted to read:

3 **CHAPTER 1057**

4 **DATA PRIVACY AND PROTECTION ACT**

5 **§9601. Short title**

6 This chapter may be known and cited as "the Data Privacy and Protection Act."

7 **§9602. Definitions**

8 As used in this chapter, unless the context otherwise indicates, the following terms
9 have the following meanings.

10 **1. Affirmative consent.** "Affirmative consent" means an affirmative act by an
11 individual that clearly communicates the individual's freely given, specific and
12 unambiguous authorization for an act or practice after having been informed, in response
13 to a specific request from a covered entity.

14 **2. Biometric information.** "Biometric information" means covered data generated
15 from the technological processing of an individual's unique biological, physical or
16 physiological characteristics that is linked or reasonably linkable to an individual.
17 "Biometric information" includes fingerprints; voice prints; iris or retina scans; facial or
18 hand mapping, geometry or templates; or gait or other unique body movements. "Biometric
19 information" does not include a digital or physical photograph; an audio or video recording;
20 or data generated from a digital or physical photograph or an audio or video recording, that
21 cannot be used, alone or in combination with other information, to identify an individual.

22 **3. Control.** "Control" means, with respect to an entity:

23 A. Ownership of, or the power to vote, more than 50% of the outstanding shares of
24 any class of voting security of the entity;

25 B. Control over the election of a majority of the directors of the entity or of individuals
26 exercising similar functions; or

27 C. The power to exercise a controlling influence over the management of the entity.

28 **4. Covered algorithm.** "Covered algorithm" means a computational process that uses
29 machine learning, natural language processing, artificial intelligence techniques or other
30 computational processing techniques of similar or greater complexity and that makes a
31 decision or facilitates human decision-making with respect to covered data, including to
32 determine the provision of products or services or to rank, order, promote, recommend,
33 amplify or similarly determine the delivery or display of information to an individual.

34 **5. Covered data.** "Covered data" means information, including derived data and
35 unique identifiers, that identifies or is linked or reasonably linkable, alone or in
36 combination with other information, to an individual or a device that identifies or is linked
37 or reasonably linkable to an individual. "Covered data" does not include de-identified data
38 or publicly available information.

1 **6. Covered entity.** "Covered entity" means a person, other than an individual acting
2 in a non-commercial context, that alone or jointly with others determines the purposes and
3 means of collecting, processing or transferring covered data. "Covered entity" includes a
4 person that controls, is controlled by or is under common control with the covered entity.
5 "Covered entity" does not include an entity that is acting as a service provider.

6 **7. Covered high-impact social media company.** "Covered high-impact social media
7 company" means a covered entity that provides an Internet-based platform that constitutes
8 an online product or service that is primarily used by users to access or share user-generated
9 content and:

10 A. Generates \$3,000,000,000 or more in annual revenue; and

11 B. Has 300,000,000 or more monthly active users for not fewer than 3 of the preceding
12 12 months on the online product or service of the covered entity.

13 **8. Covered language.** "Covered language" means one of the 10 languages with the
14 most speakers in the United States, according to the most recent United States census.

15 **9. Data broker.** "Data broker" means a covered entity whose principal source of
16 revenue is derived from processing or transferring covered data that the covered entity did
17 not collect directly from the individuals linked or linkable to the covered data. "Data
18 broker" does not include a covered entity as long as that covered entity is acting as a service
19 provider. For purposes of this subsection, "principal source of revenue" means, for the prior
20 12-month period, either more than 50% of all revenue of the covered entity or obtaining
21 revenue from processing or transferring the covered data of more than 5,000,000
22 individuals that the covered entity did not collect directly from the individuals linked or
23 linkable to the covered data.

24 **10. De-identified data.** "De-identified data" means information that does not identify
25 and is not linked or reasonably linkable to a distinct individual or a device, regardless of
26 whether the information is aggregated.

27 **11. Large data holder.** "Large data holder" means a covered entity or service provider
28 that, in the most recent calendar year, had annual gross revenues of \$250,000,000 or more
29 and collected, processed or transferred the covered data of more than 5,000,000 individuals
30 or devices that identify or are linked or reasonably linkable to one or more individuals,
31 excluding covered data collected and processed solely for the purpose of billing for,
32 finalizing or otherwise collecting payment for a requested product or service and sensitive
33 data of more than 200,000 individuals or devices that identify or are linked or reasonably
34 linkable to one or more individuals. "Large data holder" does not include an instance in
35 which the covered entity or service provider would qualify as a large data holder solely on
36 the basis of collecting or processing personal e-mail addresses, personal telephone numbers
37 or log-in information of an individual or device to allow the individual or device to log in
38 to an account administered by the covered entity or service provider.

39 **12. Material.** "Material," with respect to an act, practice or representation of a covered
40 entity, including a representation made by the covered entity in a privacy policy or similar
41 disclosure to individuals, involving the collection, processing or transfer of covered data,
42 means that the act, practice or representation is likely to affect a reasonable individual's
43 decisions, conduct or expectations regarding a product or service or processing of personal
44 data.

- 1 **13. Sensitive data.** "Sensitive data" means the following types of covered data:
- 2 A. A government-issued identifier, including a Social Security number, passport
3 number or driver's license number, that is not required by law to be displayed in public;
- 4 B. Information that describes or reveals the physical health, mental health, disability,
5 diagnosis or health condition or treatment of an individual;
- 6 C. A financial account number, debit card number, credit card number or information
7 that describes the income level or bank account balances of an individual, except that
8 "sensitive data" does not include the last 4 digits of a debit or credit card number;
- 9 D. Biometric information;
- 10 E. Genetic information;
- 11 F. Information that is derived from a device or technology that reveals the past or
12 present physical location of an individual or device that identifies or is linked or
13 reasonably linkable to one or more individuals, with sufficient precision to identify
14 street-level location information of an individual or device or the location of an
15 individual or device within a range of 1,850 feet or less, but not geolocation
16 information identifiable or derived solely from the visual content of a legally obtained
17 image, including the location of the device that captured the image;
- 18 G. An individual's private communications, including voicemails, e-mails, texts, direct
19 messages or mail, or information identifying the parties to those communications,
20 voice communications, video communications and information that pertains to the
21 transmission of those communications, including telephone numbers called, telephone
22 numbers from which calls were placed, the time calls were made, call duration and
23 location information of the parties to the call, unless the covered entity or a service
24 provider acting on behalf of the covered entity is the sender or an intended recipient of
25 the communication. For purposes of this paragraph, communications are not private if
26 those communications are made from or to a device provided by an employer to an
27 employee and the employer provides conspicuous notice that the employer may access
28 communications made on the device;
- 29 H. Account or device log-in credentials or security or access codes for an account or
30 device;
- 31 I. Information identifying the sexual behavior of an individual in a manner inconsistent
32 with the individual's reasonable expectation regarding the collection, processing or
33 transfer of that information;
- 34 J. Calendar information, address book information, phone or text logs, photos, audio
35 recordings or videos maintained for private use by an individual, regardless of whether
36 that information is stored on the individual's device or is accessible from that device
37 and is backed up in a separate location. For purposes of this paragraph, information is
38 not sensitive if the information is sent from or to a device provided by an employer to
39 an employee and the employer provides conspicuous notice that the employer may
40 access the information on the device;
- 41 K. A photograph, film, video recording or other similar medium that shows the naked
42 or undergarment-clad genitals of an individual;

1 L. Information revealing the video content requested or selected by an individual
2 collected by a covered entity, not including covered data used solely for transfers for
3 independent video measurement;

4 M. Information about an individual when the covered entity or service provider has
5 knowledge that the individual is a minor;

6 N. An individual's race, color, ethnicity, religion, employment history, immigration
7 status or union membership or information about the individual's family or social
8 relationships; and

9 O. Information identifying an individual's online activities over time and across 3rd-
10 party websites or online services.

11 **14. Service provider.** "Service provider" means a person that collects, processes or
12 transfers and receives covered data on behalf of and at the direction of a covered entity or
13 a federal, state, tribal, territorial or local government entity.

14 **15. Service provider data.** "Service provider data" means covered data that is
15 collected or processed by or has been transferred to a service provider by or on behalf of a
16 covered entity, another service provider or a federal, state, tribal, territorial or local
17 government entity for the purpose of allowing the service provider to whom the covered
18 data is transferred to perform a service or function on behalf of and at the direction of the
19 covered entity, service provider or a federal, state, tribal, territorial or local government
20 entity.

21 **16. Small business.** "Small business" means a covered entity or a service provider that
22 meets the following criteria for the period of the 3 preceding calendar years or for the period
23 during which the covered entity or service provider has been in existence if the covered
24 entity or service provider has been in existence less than 3 years:

25 A. The covered entity or service provider's average annual gross revenues during the
26 period did not exceed \$41,000,000;

27 B. The covered entity or service provider, on average, did not annually collect or
28 process the covered data of more than 200,000 individuals during the period beyond
29 the purpose of initiating, billing for, finalizing or otherwise collecting payment for a
30 requested service or product, as long as all covered data for that purpose was deleted
31 or de-identified within 90 days, except when necessary to investigate fraud or as
32 consistent with a covered entity's return policy; and

33 C. Is not a data broker.

34 **17. Substantial privacy risk.** "Substantial privacy risk" means the collection,
35 processing or transfer of covered data in a manner that may result in a reasonably
36 foreseeable substantial physical injury, economic injury, highly offensive intrusion into the
37 privacy expectations of a reasonable individual under the circumstances or discrimination
38 on the basis of race, color, religion, national origin, sex or disability.

39 **18. Targeted advertising.** "Targeted advertising" means presenting to an individual
40 or device identified by a unique identifier, or groups of individuals or devices identified by
41 unique identifiers, an online advertisement that is selected based on known or predicted
42 preferences, characteristics or interests associated with the individual or a device identified
43 by a unique identifier. "Targeted advertising" does not include advertising or marketing to

1 an individual or an individual's device in response to the individual's specific request for
2 information or feedback; an advertisement displayed based on the content or nature of the
3 publicly accessible website or service in which the advertisement appears and does not vary
4 based on who is viewing the advertisement; or processing covered data strictly necessary
5 for the sole purpose of measuring or reporting advertising or content, performance, reach
6 or frequency, including independent measurement.

7 **19. Third party.** "Third party" means a person, including a covered entity, that
8 collects, processes or transfers covered data and is not a consumer-facing business with
9 which the individual linked or reasonably linkable to that covered data expects and intends
10 to interact and is not a service provider with respect to that data. "Third party" does not
11 include a person that collects covered data from another entity if the 2 entities are related
12 by common ownership or corporate control unless a reasonable consumer's reasonable
13 expectation would be that the entities share information.

14 **§9603. Applicability**

15 This chapter does not apply to:

16 **1. Government agencies.** A government agency or service provider to a government
17 agency that exclusively and solely processes information provided by government entities;
18 or

19 **2. Certain persons.** A person that meets the following criteria for the period of the 3
20 preceding calendar years or for the period during which the person has been in existence if
21 the person is an entity that has been in existence for less than 3 years:

22 A. The person's average annual gross revenues during the period did not exceed
23 \$20,000,000;

24 B. The person, on average, did not annually collect or process the covered data of more
25 than 75,000 individuals during the period beyond the purpose of initiating, billing for,
26 finalizing or otherwise collecting payment for a requested service or product, as long
27 as all covered data for that purpose was deleted or de-identified within 90 days, except
28 when necessary to investigate fraud or as consistent with a covered entity's return
29 policy; and

30 C. No component of the person's revenue comes from transferring covered data during
31 a year or part of a year if the person is an entity that has been in existence for less than
32 one year.

33 **§9604. Actions regarding covered data**

34 **1. Prohibitions.** Except as provided by subsection 2, a covered entity may not collect,
35 process or transfer covered data unless the collection, processing or transfer is limited to
36 what is reasonably necessary and proportionate to provide or maintain a specific product
37 or service requested by the individual to whom the data pertains. A covered entity or
38 service provider may not engage in deceptive advertising or marketing with respect to a
39 product or service offered to an individual.

40 **2. Allowed purposes.** A covered entity may collect, process or transfer covered data
41 for any of the following purposes if the collection, processing or transfer is limited to what
42 is reasonably necessary and proportionate to that purpose:

- 1 A. To initiate, manage or complete a transaction or fulfill an order for a specific
2 product or service requested by an individual, including associated routine
3 administrative, operational and account-servicing activity including billing, shipping,
4 delivery, storage and accounting;
- 5 B. With respect to covered data previously collected in accordance with this chapter:
- 6 (1) To process the data as necessary to perform system maintenance or diagnostics;
7 (2) To develop, maintain, repair or enhance a product or service for which the data
8 was collected;
9 (3) To conduct internal research or analytics to improve a product or service for
10 which the data was collected;
11 (4) To perform inventory management or reasonable network management;
12 (5) To protect against spam;
13 (6) To debug or repair errors that impair the functionality of a service or product
14 for which the data was collected;
15 (7) To process the data as necessary to provide first-party advertising or marketing
16 of products or services provided by the covered entity for individuals who are not
17 minors. For purposes of this subparagraph, "first-party advertising or marketing"
18 means advertising or marketing conducted by a covered entity that collects covered
19 data from the individual linked or reasonably linkable to that data through either
20 direct communications with the individual including direct mail, e-mail or text
21 message communications, or advertising or marketing conducted entirely within
22 the first-party context, including in a physical location operated by or on behalf of
23 the covered entity, or on a website or mobile application operated by or on behalf
24 of the covered entity; and
25 (8) To provide targeted advertising;
- 26 C. To authenticate users of a product or service;
- 27 D. To fulfill a product or service warranty;
- 28 E. To prevent, detect, protect against or respond to a security incident. For purposes
29 of this paragraph, "security incident" means a network security or physical security
30 incident, including an intrusion or trespass, medical alert or fire alarm;
- 31 F. To prevent, detect, protect against or respond to fraud, harassment or illegal activity
32 targeted at or involving the covered entity or its services. For purposes of this
33 paragraph, the term "illegal activity" means a violation of a federal, state or local law
34 punishable as a crime that can directly cause harm to another person;
- 35 G. To comply with a legal obligation imposed by federal, tribal, local or state law or
36 to investigate, establish, prepare for or defend legal claims involving the covered entity
37 or service provider;
- 38 H. To prevent an individual from suffering harm when the covered entity or service
39 provider believes in good faith that the individual is at risk of death, serious physical
40 injury or other serious health risk;
- 41 I. To carry out a product recall pursuant to federal or state law;

1 J. To conduct a public or peer-reviewed scientific, historical or statistical research
2 project that:

3 (1) Is in the public interest; and

4 (2) Adheres to all relevant laws and regulations governing that research, including
5 regulations for the protection of human subjects, or is excluded from criteria of the
6 institutional review board;

7 K. To deliver a communication that is not an advertisement to an individual, if the
8 communication is reasonably anticipated by the individual within the context of the
9 individual's interactions with the covered entity;

10 L. To deliver a communication at the direction of an individual between that individual
11 and one or more individuals or entities;

12 M. To transfer assets to a 3rd party in the context of a merger, acquisition, bankruptcy
13 or similar transaction when the 3rd party assumes control, in whole or in part, of the
14 covered entity's assets, only if the covered entity, in a reasonable time prior to the
15 transfer, provides an affected individual with:

16 (1) A notice describing the transfer, including the name of the entity receiving the
17 individual's covered data and the applicable privacy policies; and

18 (2) A reasonable opportunity to withdraw previously given consent in accordance
19 with the requirements of affirmative consent under section 9609 related to the
20 individual's covered data and a reasonable opportunity to request the deletion of
21 the individual's covered data;

22 N. To ensure the data security and integrity of covered data; and

23 O. To support or promote participation by individuals in civic engagement activities
24 and democratic governance, including voting, petitioning, engaging with government
25 proceedings, providing indigent legal aid services and unionizing.

26 **§9605. Actions regarding sensitive data**

27 A covered entity or service provider may not:

28 **1. Social security numbers.** Process or transfer a social security number, except when
29 necessary to facilitate an extension of credit, authentication, fraud and identity fraud
30 detection and prevention, the payment or collection of taxes, the enforcement of a contract
31 between parties or the prevention, investigation or prosecution of fraud or illegal activity
32 or as otherwise required by federal, state or local law;

33 **2. Collections and processing.** Collect or process sensitive data, except when the
34 collection or processing is strictly necessary to provide or maintain a specific product or
35 service requested by the individual to whom the sensitive data pertains or is strictly
36 necessary to achieve a purpose described by section 9604, subsection 2, paragraphs A to
37 N;

38 **3. Third parties.** Transfer an individual's sensitive data to a 3rd party, unless:

39 A. The transfer is made with the affirmative consent of the individual;

40 B. The transfer is necessary to comply with a legal obligation imposed by federal,
41 state, tribal or local law or to investigate, establish, exercise or defend legal claims;

1 C. The transfer is necessary to prevent an individual from imminent injury when the
2 covered entity believes in good faith that the individual is at risk of death, serious
3 physical injury or serious health risk;

4 D. In the case of the transfer of a password, the transfer is necessary to use a designated
5 password manager or the transfer is to a covered entity for the exclusive purpose of
6 identifying passwords that are being reused across sites or accounts;

7 E. In the case of the transfer of genetic information, the transfer is necessary to perform
8 a medical diagnosis or medical treatment specifically requested by an individual or to
9 conduct medical research; or

10 F. The transfer complies with section 9604, subsection 2, paragraph M;

11 **4. Communication services.** In the case of a provider of broadcast television service,
12 cable service, satellite service, streaming media service or other video programming service
13 described in 47 United States Code, Section 613(h)(2), transfer to an unaffiliated 3rd party
14 covered data that reveals the video content or services requested or selected by an
15 individual from that service, except with the affirmative consent of the individual or
16 pursuant to one of the permissible purposes listed in subsection 2; or

17 **5. Targeted advertising.** Process sensitive data for the purposes of targeted
18 advertising.

19 **§9606. Policies, practices and procedures**

20 **1. Required policies, practices and procedures.** A covered entity and a service
21 provider shall establish, implement and maintain reasonable policies, practices and
22 procedures that reflect the role of the covered entity or service provider in the collection,
23 processing and transferring of covered data and that:

24 A. Consider applicable federal and state laws, rules or regulations related to covered
25 data that the covered entity or service provider collects, processes or transfers;

26 B. Identify, assess and mitigate privacy risks related to minors;

27 C. Mitigate privacy risks, including substantial privacy risks, related to the products
28 and services of the covered entity or the service provider, including in the design,
29 development and implementation of those products and services, taking into account
30 the role of the covered entity or service provider and the information available to it;
31 and

32 D. Implement reasonable training and safeguards within the covered entity and service
33 provider to promote compliance with all privacy laws applicable to covered data the
34 covered entity collects, processes or transfers or covered data the service provider
35 collects, processes or transfers on behalf of the covered entity and mitigate privacy
36 risks, including substantial privacy risks, taking into account the role of the covered
37 entity or service provider and the information available to it.

38 **2. Requirements.** The policies, practices and procedures established by a covered
39 entity and a service provider under subsection 1, must take into account, as applicable:

40 A. The size of the covered entity or service provider and the nature, scope and
41 complexity of the activities engaged in by the covered entity or service provider,
42 including whether the covered entity or service provider is a large data holder,

- 1 nonprofit organization, small business, 3rd party or data broker, taking into account the
- 2 role of the covered entity or service provider and the information available to the
- 3 covered entity or service provider;
- 4 B. The sensitivity of the covered data collected, processed or transferred by the
- 5 covered entity or service provider;
- 6 C. The volume of covered data collected, processed or transferred by the covered entity
- 7 or service provider;
- 8 D. The number of individuals and devices to which the covered data collected,
- 9 processed or transferred by the covered entity or service provider relates; and
- 10 E. The cost of implementing those policies, practices and procedures in relation to the
- 11 risks and nature of the covered data.

12 **§9607. Prohibition on retaliation against an individual for exercise of rights and**

13 **unlawful pricing**

14 **1. Retaliation prohibited.** A covered entity may not retaliate against an individual for

15 exercising a right guaranteed by this chapter or by a rule adopted under this chapter or for

16 refusing to agree to the collection or processing of covered data for a separate product or

17 service. For purposes of this subsection, retaliation includes denying goods or services,

18 charging different prices or rates for goods or services or providing a different level of

19 quality of goods or services.

20 **2. Unlawful pricing prohibited.** A covered entity may not offer different types of

21 pricing that are unjust, unreasonable, coercive or usurious in nature.

22 **3. Interpretation.** Subsection 1 may not be construed to:

23 A. Prohibit the relation of the price of a service or the level of service provided to an

24 individual to the provision, by the individual, of financial information that is

25 necessarily collected and processed only for the purpose of initiating, billing for or

26 collecting payment for a service or product requested by the individual;

27 B. Prohibit a covered entity from offering a different price, rate, level, quality or

28 selection of goods or services to an individual, including offering goods or services for

29 no fee, if the offering is in connection with an individual's voluntary participation in a

30 bona fide loyalty, rewards, premium features, discount or club card program, as long

31 as the covered entity may not transfer covered data to a 3rd party as part of a program

32 unless:

33 (1) The transfer is reasonably necessary to enable the 3rd party to provide a benefit

34 to which the individual is entitled;

35 (2) The transfer of covered data to the 3rd party is clearly disclosed in the terms

36 of the program; and

37 (3) The 3rd party uses the covered data only for purposes of facilitating a benefit

38 to which the individual is entitled and does not retain or otherwise use or disclose

39 the covered data for any other purpose;

40 C. Require a covered entity to provide a bona fide loyalty program that would require

41 the covered entity to collect, process or transfer covered data that the covered entity

42 otherwise would not collect, process or transfer;

1 D. Prohibit a covered entity from offering a financial incentive or other consideration
2 to an individual for participation in the collection, processing or transfer of covered
3 data as reasonably necessary and proportionate to investigate the market for or
4 marketing of products, services or ideas, when the covered data is not integrated into a
5 product or service otherwise used to contact an individual or individual's device or used
6 to advertise or market to an individual or individual's device;

7 E. Prohibit a covered entity from offering different types of pricing or functionalities
8 with respect to a product or service based on an individual's exercise of a right; or

9 F. Prohibit a covered entity from declining to provide a product or service insofar as
10 the collection and processing of covered data is strictly necessary for that product or
11 service.

12 **§9608. Privacy policy**

13 **1. Privacy policy required.** A covered entity or service provider shall make publicly
14 available, in a clear, conspicuous and readily accessible manner, a privacy policy that
15 provides a detailed and accurate representation of the data collection, processing and
16 transfer activities of the covered entity. The policy must be provided in a manner that is
17 reasonably accessible to and usable by individuals with disabilities. The covered entity or
18 service provider shall make the policy available to the public in each covered language in
19 which the covered entity or service provider provides a product or service that is subject to
20 the privacy policy or carries out activities related to that product or service. The policy must
21 include, at a minimum, the following:

22 A. The identity and the contact information of:

23 (1) The covered entity or service provider to which the privacy policy applies,
24 including the covered entity's or service provider's points of contact and general e-
25 mail addresses, as applicable, for privacy and data security inquiries; and

26 (2) Another entity within the same corporate structure as the covered entity or
27 service provider to which covered data is transferred by the covered entity;

28 B. The categories of covered data that the covered entity or service provider collects
29 or processes;

30 C. The processing purposes for each category of covered data the covered entity or
31 service provider collects or processes;

32 D. Whether the covered entity or service provider transfers covered data and, if so,
33 each category of service provider and 3rd party to which the covered entity or service
34 provider transfers covered data; the name of each data broker to which the covered
35 entity or service provider transfers covered data; and the purposes for which the data
36 is transferred to the categories of service providers and 3rd parties except for a transfer
37 to a governmental entity pursuant to a court order or law that prohibits the covered
38 entity or service provider from disclosing the transfer;

39 E. The length of time the covered entity or service provider intends to retain each
40 category of covered data, including sensitive covered data, or, if it is not possible to
41 identify the length of time, the criteria used to determine the length of time the covered
42 entity or service provider intends to retain categories of covered data;

1 F. A prominent description of how an individual can exercise the rights described in
2 this chapter;

3 G. A general description of the covered entity's or service provider's data security
4 practices; and

5 H. The effective date of the privacy policy.

6 **2. Changes to privacy policies.** If a covered entity makes a material change to its
7 privacy policy, the covered entity shall notify each individual affected by the material
8 change before implementing the material change with respect to prospectively collected
9 covered data and, except as provided in subsection 9604, subsection 2, provide a reasonable
10 opportunity for each individual to withdraw consent to further materially different
11 collection, processing or transfer of previously collected covered data under the changed
12 policy. The covered entity shall take all reasonable electronic measures to provide direct
13 notification regarding material changes to the privacy policy to each affected individual, in
14 each covered language in which the privacy policy is made available, and taking into
15 account available technology and the nature of the relationship.

16 **3. Large data holders.** A large data holder shall retain copies of previous versions of
17 its privacy policy for at least 10 years beginning after the effective date of this chapter and
18 publish them on the large data holder's publicly accessible website. A large data holder
19 shall make publicly available, in a clear, conspicuous and readily accessible manner, a log
20 describing the date and nature of each material change to its privacy policy over the past
21 10 years. The descriptions must be sufficient for a reasonable individual to understand the
22 effect of each material change. The obligations in this subsection do not apply to a previous
23 version of a large data holder's privacy policy or a material change to a privacy policy that
24 precede the effective date of this chapter.

25 In addition to the privacy policy required under subsection 1, a large data holder that is a
26 covered entity shall provide a short-form notice of its covered data practices in a manner
27 that is:

28 A. Concise, clear, conspicuous and not misleading;

29 B. Readily accessible to the individual, based on what is reasonably anticipated within
30 the context of the relationship between the individual and the large data holder;

31 C. Inclusive of an overview of individual rights and disclosures to draw attention to
32 data practices that may be unexpected to a reasonable person or that involve sensitive
33 covered data; and

34 D. Not more than 500 words in length.

35 **§9609. Affirmative consent**

36 **1. Valid consent.** An expression of consent in response to a request from a covered
37 entity or service provider is not affirmative consent for purposes of this chapter unless the
38 individual gives consent under the following conditions:

39 A. The request is provided to the individual in a clear and conspicuous stand-alone
40 disclosure made through the primary medium used to offer the covered entity's product
41 or service, or, if the product or service is not offered in a medium that permits the
42 making of the request under this paragraph, another medium regularly used in
43 conjunction with the covered entity's product or service;

1 B. The request includes a description of the processing purpose for which the
2 individual's consent is sought and:

3 (1) Clearly states the specific categories of covered data that the covered entity
4 intends to collect, process or transfer necessary to achieve the processing purpose;
5 and

6 (2) Includes a prominent heading and is written in language that would enable a
7 reasonable individual to identify and understand the processing purpose for which
8 consent is sought and the covered data to be collected, processed or transferred by
9 the covered entity for the processing purpose;

10 C. The request clearly explains the individual's rights related to consent;

11 D. The request is made in a manner reasonably accessible to and usable by individuals
12 with disabilities;

13 E. The request is made available to the individual in each covered language in which
14 the covered entity provides a product or service for which authorization is sought;

15 F. The option to refuse to give consent is at least as prominent as the option to give
16 consent and the option to refuse to give consent takes the same number of steps or
17 fewer as the option to give consent; and

18 G. Affirmative consent to an act or practice is not inferred from the inaction of the
19 individual or the individual's continued use of a service or product provided by the
20 covered entity.

21 **2. Prohibitions.** A covered entity or service provider may not obtain or attempt to
22 obtain affirmative consent through:

23 A. The use of a false, fraudulent or materially misleading statement or representation;
24 or

25 B. The design, modification or manipulation of a user interface with the purpose or
26 substantial effect of obscuring, subverting or impairing a reasonable individual's choice
27 to provide consent or covered data.

28 **3. Different processing purpose.** Processing or transferring of covered data collected
29 pursuant to affirmative consent for a different processing purpose than that for which
30 affirmative consent was obtained requires affirmative consent for the subsequent
31 processing purpose.

32 **4. Withdrawal of consent.** A covered entity shall provide an individual with a clear
33 and conspicuous means to withdraw affirmative consent previously provided by the
34 individual that is as easy to execute by a reasonable individual as the means to provide
35 consent.

36 **5. Opt out.** A covered entity may not transfer or direct the transfer of the covered data
37 of an individual to a 3rd party unless the individual provides affirmative consent and shall
38 provide an opportunity for an individual to object to a transfer through an opt-out
39 mechanism. A covered entity is not required to provide an individual an opportunity to opt
40 out of the collection, processing or transfer of covered data made pursuant to section 9604,
41 subsection 2.

42 **§9610. Targeted advertising**

1 **1. Affirmative consent required.** Before engaging in targeted advertising to an
2 individual or device, a covered entity or service provider that directly delivers a targeted
3 advertisement shall obtain the individual's affirmative consent for targeted advertising. The
4 covered entity or service provider shall provide an opportunity for an individual to make
5 an opt-out designation with respect to targeted advertising. The covered entity or service
6 provider shall abide by an opt-out designation made by the individual with respect to
7 targeted advertising. A covered entity or service provider that receives an opt-out
8 designation made by an individual shall notify any other person that directed the covered
9 entity or service provider to serve, deliver or otherwise handle the advertisement of the opt-
10 out designation.

11 **2. Prohibitions.** A covered entity may not engage in targeted advertising to an
12 individual if the covered entity:

13 A. Is a covered high-impact social media company and knew or should have known
14 the individual was a minor at the time of the advertising;

15 B. Is a large data holder and not a covered high-impact social media company and
16 knew or acted in willful disregard of the fact that the individual was a minor at the time
17 of the advertising; or

18 C. Has knowledge that the individual was a minor at the time of the advertising.

19 **§9611. Individual rights regarding covered data**

20 **1. Access.** Except as provided by this section, after receiving a request from an
21 individual, a covered entity shall:

22 A. Provide that individual with access to:

23 (1) The individual's covered data, except covered data in a backup or archival
24 system, that is collected, processed or transferred by the covered entity or a service
25 provider of the covered entity within the 24 months preceding the request, in a
26 format that a reasonable individual can understand and download from the Internet;
27 and

28 (2) If applicable:

29 (a) The categories of 3rd parties to which the covered entity has transferred
30 for consideration the covered data of the individual;

31 (b) An option for consumers to obtain the names of 3rd parties or service
32 providers to which the covered entity has transferred for consideration the
33 covered data of the individual;

34 (c) The categories of sources from which the covered data was collected; and

35 (d) A description of the purpose for which the covered entity transferred the
36 covered data of the individual to a 3rd party or service provider;

37 B. Correct a verifiable substantial inaccuracy or substantially incomplete information
38 with respect to the covered data of the individual that is processed by the covered entity
39 and make reasonable efforts to notify all 3rd parties or service providers to which the
40 covered entity transferred the covered data of the corrected information. A small
41 business may delete the relevant information instead of making a correction;

1 C. Delete covered data of the individual that is processed by the covered entity and
2 make reasonable efforts to notify all 3rd parties or service providers to which the
3 covered entity transferred the covered data of the individual's deletion request; and

4 D. To the extent technically feasible, export to the individual or directly to another
5 entity the covered data of the individual that is processed by the covered entity,
6 including inferences linked or reasonably linkable to the individual but not including
7 derived data:

8 (1) Without licensing restrictions that limit transfers;

9 (2) In a format that a reasonable individual can understand and download from the
10 Internet; and

11 (3) In a portable, structured, interoperable and machine-readable format.

12 A small business is not required to comply with subparagraph (2) or (3).

13 **2. Conditions.** A covered entity may not condition, effectively condition, attempt to
14 condition or attempt to effectively condition an action required in subsection 1 through:

15 A. The use of a false, fraudulent or materially misleading statement or representation;
16 or

17 B. The design, modification or manipulation of a user interface with the purpose or
18 substantial effect of obscuring, subverting or impairing a reasonable individual's
19 choice.

20 **3. Response periods.** A covered entity or service provider shall comply with a request
21 to perform an action under subsection 1 within the following response periods:

22 A. For a large data holder, no later than the 45th day after the date of the request by an
23 individual, unless it is demonstrably impracticable or impracticably costly to verify the
24 identity of the individual; or

25 B. For a covered entity that is not a large data holder, no later than the 60th day after
26 the date of the request by an individual, unless it is demonstrably impracticable or
27 impracticably costly to verify the identity of the individual.

28 A response period described in this subsection may be extended once by 45 additional days
29 when reasonably necessary, considering the complexity and number of the individual's
30 requests, as long as the covered entity informs the individual of the extension within the
31 initial 45-day or 60-day response period, together with the reason for the extension.

32 **4. Multiple requests from one individual.** A covered entity shall perform the actions
33 described in subsection 1 free of charge with respect to the first 2 times that an individual
34 makes a request in a 12-month period. Beyond the first 2 requests in a 12-month period,
35 the covered entity or service provider may charge a reasonable fee for each request.

36 **5. Verification.** If a covered entity cannot reasonably verify that a request to take an
37 action under subsection 1 is made by the individual whose covered data is the subject of
38 the request, or an individual authorized to make a request on the individual's behalf, the
39 covered entity:

40 A. May request that the individual making the request provide additional information
41 necessary for the sole purpose of verifying the identity of the individual; and

1 B. May not process or transfer additional information provided under paragraph A for
2 any other purpose.

3 **6. Exceptions.** A covered entity is not required to take an action described by
4 subsection 1 if:

5 A. The covered entity cannot reasonably verify that the individual making the request
6 is the individual whose covered data is the subject of the request or an individual
7 authorized to make a request on the individual's behalf;

8 B. The covered entity reasonably believes that:

9 (1) The request is made to interfere with a contract between the covered entity and
10 another individual;

11 (2) The action would require the covered entity to engage in an unfair or deceptive
12 practice under 15 United States Code, Section 45 or state law; or

13 (3) The request is made to further fraud or support criminal activity or the action
14 presents a data security threat;

15 C. The covered entity determines that the action would require access to or correction
16 of another individual's sensitive data; or

17 D. The action:

18 (1) Requires the covered entity to retain covered data collected for a single, one-
19 time transaction, if that covered data is not processed or transferred by the covered
20 entity for any purpose other than completing the transaction;

21 (2) Is demonstrably impracticable or prohibitively costly to take, in which case the
22 covered entity shall provide a description to the requestor detailing the inability to
23 comply with the request. The receipt of a large number of verified requests, on its
24 own, may not be considered to render compliance with a request demonstrably
25 impracticable;

26 (3) Requires the covered entity to attempt to re-identify de-identified data;

27 (4) Requires the covered entity to maintain covered data in an identifiable form or
28 collect, retain or access data in order to be capable of associating a request with the
29 covered data of the individual who made the request;

30 (5) Would result in the release of privileged or confidential business information;

31 (6) Requires the covered entity to correct covered data that cannot be reasonably
32 verified as being inaccurate or incomplete;

33 (7) Violates federal or state law or the rights of another individual, including the
34 rights under the United States Constitution;

35 (8) Prevents a covered entity from being able to maintain a confidential record of
36 deletion requests, maintained solely for the purpose of preventing covered data of
37 an individual from being recollected after the individual submitted a deletion
38 request and requested that the covered entity no longer collect, process or transfer
39 the data; or

40 (9) With respect to a request for deletion:

- 1 (a) Would unreasonably interfere with the provision of products or services
- 2 by the covered entity to another person it currently serves;
- 3 (b) Would require the deletion of covered data that relates to a public figure,
- 4 public official or limited-purpose public feature and for which the requesting
- 5 individual has no reasonable expectation of privacy with respect to that
- 6 covered data;
- 7 (c) Would require the deletion of covered data reasonably necessary to
- 8 perform a contract between the covered entity and the individual;
- 9 (d) Would require the deletion of covered data that the covered entity needs
- 10 to retain in order to comply with professional ethical obligations;
- 11 (e) Would require the deletion of covered data that the covered entity
- 12 reasonably believes may be evidence of unlawful activity or an abuse of the
- 13 covered entity's products or services; or
- 14 (f) For private elementary and secondary schools and private institutions of
- 15 higher education as defined by Title I of the federal Higher Education Act of
- 16 1965, would require the deletion of covered data that would unreasonably
- 17 interfere with the provision of education services by or the ordinary operation
- 18 of the school or institution.

19 With respect to a request that is subject to an exception described by this subsection, a

20 covered entity shall partially comply with the remainder of the request if it is possible and

21 not unduly burdensome to do so.

22 **7. Languages.** A covered entity shall provide an opportunity to make a request under

23 this section in a covered language in which the covered entity provides a product or service.

24 The mechanisms by which a covered entity enables individuals to make requests under this

25 section must be readily accessible and usable by individuals with disabilities.

26 **8. Transfer of certain covered data.** A covered entity may not transfer or direct the

27 transfer of the covered data of a minor to a 3rd party if the covered entity has knowledge

28 that the individual is a minor and has not obtained affirmative consent from the minor or

29 the minor's parent or guardian. A covered entity or service provider may collect, process

30 or transfer covered data of an individual the covered entity or service provider knows is a

31 minor in order to submit information relating to child victimization to law enforcement

32 agencies or to the nonprofit, national resource center and clearinghouse designated by the

33 United States Congress to assist victims, families, child-serving professionals and the

34 general public on issues pertaining to missing and exploited children.

35 **§9612. Requirements for large data holders**

36 **1. Reporting required.** For each calendar year in which it was a large data holder, a

37 covered entity shall:

- 38 A. Compile the following metrics for the prior calendar year:
- 39 (1) The number of verified requests to access information;
- 40 (2) The number of verified requests to delete information;
- 41 (3) The number of requests to opt out of covered data transfers;
- 42 (4) The number of requests to opt out of targeted advertising;

1 (5) The number of requests under subparagraphs (1) to (4) that the large data
2 holder complied with in whole or in part or denied; and

3 (6) The median and mean number of days within which the large data holder
4 substantively responded to the requests under subparagraphs (1) to (4); and

5 B. Disclose by July 1st of each applicable calendar year the information compiled in
6 paragraph A within the large data holder's privacy policy or on the publicly accessible
7 website of the large data holder that is accessible from a hyperlink included in the
8 privacy policy.

9 **2. Certification.** An executive officer of a large data holder shall certify annually, in
10 good faith, to the Attorney General that the entity maintains:

11 A. Internal controls reasonably designed to comply with this chapter; and

12 B. Internal reporting structures to ensure that the certifying executive officer is
13 involved in and responsible for the decisions that impact the compliance by the large
14 data holder with this chapter.

15 A certification submitted under this subsection must be based on a review of the
16 effectiveness of the internal controls and reporting structures of the large data holder that
17 is conducted by the certifying executive officer not earlier than the 90th day before the date
18 of the submission of the certification. A certification is made in good faith if the certifying
19 executive officer, after a reasonable investigation, had reasonable grounds to believe and
20 did believe, at the time that certification was submitted, that the statements in the
21 certification were true and that there was no omission of a material fact or a fact necessary
22 to make the statements in the certification not misleading.

23 **§9613. Data brokers**

24 **1. Notice required.** A data broker shall place a clear, conspicuous, not misleading and
25 readily accessible notice on the publicly accessible website or mobile application of the
26 data broker that notifies individuals that the entity is a data broker and includes a link to a
27 website through which an individual may easily exercise the rights provided under this
28 chapter.

29 **2. Registration required.** No later than January 31st of each calendar year that follows
30 a calendar year during which a covered entity acted as a data broker and processed covered
31 data pertaining to more than 5,000 individuals or devices that identify or are linked or
32 reasonably linkable to an individual, the covered entity shall register with the Attorney
33 General in accordance with this subsection. In registering with the Attorney General, a data
34 broker shall:

35 A. Pay to the Attorney General a registration fee of \$100; and

36 B. Provide the Attorney General with the following information:

37 (1) The legal name and primary physical mailing address, e-mail address and
38 publicly accessible website address of the data broker;

39 (2) A description of the categories of covered data the data broker processes and
40 transfers;

1 (3) The contact information of the data broker, including a contact person, a
2 telephone number, an e-mail address, a publicly accessible website address and a
3 physical mailing address.

4 The Attorney General shall establish and maintain on a publicly accessible website a
5 searchable central registry of data brokers that are registered with the Attorney General.

6 A data broker that fails to register or provide the notice as required under this subsection is
7 liable for a civil penalty of \$100 for each day the data broker fails to register or provide
8 notice as required under this subsection, not to exceed a total of \$10,000 per year, and an
9 amount equal to the registration fees due under this section for each year that the data broker
10 failed to register as required pursuant to this section.

11 **§9614. Discrimination prohibited**

12 **1. Discrimination prohibited.** A covered entity or a service provider may not collect,
13 process or transfer covered data in a manner that discriminates against individuals, or
14 otherwise makes unavailable the equal enjoyment of goods or services, on the basis of race,
15 color, religion, national origin, sex or disability.

16 **2. Exceptions.** This section does not apply to:

17 A. The collection, processing or transfer of covered data for the purpose of:

18 (1) A covered entity's or a service provider's self-testing to prevent or mitigate
19 unlawful discrimination; or

20 (2) Diversifying an applicant, participant or customer pool; or

21 B. A private establishment, as described in 42 United States Code, Section 2000a(e).

22 **§9615. Algorithms**

23 **1. Assessment required.** A covered entity that is not a small business and that uses a
24 covered algorithm in a manner that poses a consequential risk of harm to an individual or
25 group of individuals and uses the covered algorithm solely or in part to collect, process or
26 transfer covered data or publicly available data annually shall conduct an impact
27 assessment of the algorithm. The impact assessment must include the following
28 information:

29 A. A detailed description of the design process and methodologies of the covered
30 algorithm;

31 B. A statement of the purpose and reasonably foreseeable uses of the covered
32 algorithm;

33 C. The types of data used by the covered algorithm, including the specific categories
34 and sources of data that will be processed as input and data used to train the model that
35 the covered algorithm relies on, if applicable;

36 D. A description of the outputs produced by the covered algorithm;

37 E. An assessment of the necessity and proportionality of the covered algorithm in
38 relation to its stated purpose;

39 F. A detailed description of steps the covered entity has taken or will take to mitigate
40 potential harm from the covered algorithm to an individual or group of individuals,
41 including steps related to:

- 1 (1) Minors;
- 2 (2) Making or facilitating advertising for, determining access to or restrictions on
- 3 the use of housing, education, employment, healthcare, insurance or credit
- 4 opportunities;
- 5 (3) Determining access to or restrictions on the use of a place of public
- 6 accommodation, particularly as the harm relates to the protected characteristics of
- 7 individuals, including race, color, religion, national origin, sex or disability;
- 8 (4) Disparate impact on the basis of individuals' race, color, religion, national
- 9 origin, sex or disability status; or
- 10 (5) Disparate impact on the basis of individuals' political party registration status;
- 11 and

12 G. Any other information as required by the Attorney General.

13 **2. Design evaluation.** A covered entity or service provider that develops a covered

14 algorithm that is designed to collect, process or transfer covered data shall perform, before

15 deploying the covered algorithm, an algorithmic design evaluation to evaluate the design,

16 structure and inputs of the covered algorithm, including training data used to develop the

17 covered algorithm, to reduce the risk of the potential harms identified under this section.

18 **3. Focus.** In complying with this section, a covered entity and a service provider may

19 focus the impact assessment or evaluation on a covered algorithm, or portions of a covered

20 algorithm, that will be put to use and may reasonably contribute to the risk of the potential

21 harms identified under this section.

22 **4. Report.** No later than 30 days after completing an impact assessment or evaluation

23 under this section, a covered entity or a service provider shall submit a report of the impact

24 assessment or evaluation to the Attorney General. The report must include a summary of

25 the impact assessment or evaluation and the covered entity or service provider shall make

26 the summary publicly available in a place that is easily accessible to consumers. Covered

27 entities and service providers may redact a trade secret, as defined in 18 United States Code,

28 Section 1839(3), or other confidential or proprietary information, from the report.

29 **§9616. Data security**

30 **1. Practices and procedures.** A covered entity or service provider shall establish,

31 implement and maintain reasonable administrative, technical and physical data security

32 practices and procedures to protect covered data against unauthorized access. The practices

33 must be appropriate to:

- 34 A. The size and complexity of the covered entity or service provider;
- 35 B. The nature and scope of the covered entity or the service provider's collecting,
- 36 processing or transferring of covered data;
- 37 C. The volume and nature of the covered data collected, processed or transferred by
- 38 the covered entity or service provider;
- 39 D. The sensitivity of the covered data collected, processed or transferred;
- 40 E. The current state-of-the-art administrative, technical and physical safeguards for
- 41 protecting covered data; and

1 F. The cost of available tools to improve security and reduce vulnerabilities to
2 unauthorized access of covered data in relation to the risks and nature of the covered
3 data.

4 **2. Requirements.** The data security practices of the covered entity and of the service
5 provider required under this subsection must include, for the respective entity's own
6 system, at a minimum, the following practices:

7 A. Identifying and assessing internal and external risk to the security of each system
8 maintained by the covered entity that collects, processes or transfers covered data, or
9 service provider that collects, processes or transfers covered data on behalf of the
10 covered entity;

11 B. With respect to large data holders, a plan to receive and reasonably respond to
12 unsolicited reports of vulnerabilities by an entity or individual by performing a
13 reasonable investigation of those reports;

14 C. Taking preventive and corrective action designed to mitigate reasonably foreseeable
15 risks or vulnerabilities to covered data identified by the covered entity or service
16 provider, consistent with the nature of the risk or vulnerability and the entity's role in
17 collecting, processing or transferring the data. Corrective action may include
18 implementing administrative, technical or physical safeguards or changes to data
19 security practices or the architecture, installation or implementation of network or
20 operating software;

21 D. Disposing of covered data in accordance with a retention schedule that requires the
22 deletion of covered data when the data is required to be deleted by law or is no longer
23 necessary for the purpose for which the data was collected, processed or transferred,
24 unless an individual has provided affirmative consent to that retention. Disposal may
25 include destroying, permanently erasing or otherwise modifying the covered data to
26 make the data permanently unreadable or indecipherable and unrecoverable to ensure
27 ongoing compliance with this section. A service provider shall establish practices to
28 delete or return covered data to a covered entity as requested at the end of the provision
29 of services unless retention of the covered data is required by law;

30 E. Training each employee with access to covered data on how to safeguard covered
31 data and updating the training as necessary;

32 F. Designating an officer or employee to maintain and implement the practices
33 described in this subsection; and

34 G. Implementing procedures to detect, respond to or recover from security incidents,
35 including breaches.

36 A small business is not required to comply with paragraph E, F or G.

37 **§9617. Officers**

38 **1. Privacy and data security officers required.** A covered entity or service provider
39 that is not a small business shall designate at least one qualified employee as a privacy
40 officer and at least one qualified employee as a data security officer.

41 **2. Privacy officer and data security officer duties.** An employee who is designated
42 by a covered entity or a service provider as a privacy officer or a data security officer shall,
43 at a minimum:

1 A. Implement a data privacy program and data security program to safeguard the
2 privacy and security of covered data in compliance with the requirements of this
3 chapter; and

4 B. Facilitate the covered entity or service provider's ongoing compliance with this
5 chapter.

6 **3. Large data holders.** A large data holder shall designate at least one of the officers
7 described in subsection 1 to report directly to the highest official at the large data holder as
8 a privacy protection officer who, in addition to the requirements in subsection 2, either
9 directly or through a supervised designee, shall:

10 A. Establish processes to periodically review and update the privacy and security
11 policies, practices and procedures of the large data holder, as necessary;

12 B. Conduct biennial and comprehensive audits to ensure that the policies, practices
13 and procedures of the large data holder ensure the large data holder is in compliance
14 with this chapter and ensure the audits are accessible to the Attorney General upon
15 request;

16 C. Develop a program to educate and train employees about compliance requirements
17 of this chapter;

18 D. Maintain updated, accurate, clear and understandable records of all material privacy
19 and data security practices undertaken by the large data holder; and

20 E. Serve as the point of contact between the large data holder and enforcement
21 authorities.

22 **4. Privacy impact assessment.** A covered entity that is not a small business shall
23 conduct a privacy impact assessment every other year. The assessment must weigh the
24 benefits of the covered entity's covered data collecting, processing and transfer practices
25 that may cause a substantial privacy risk against the potential material adverse
26 consequences of the practices to individual privacy. The covered entity shall make a
27 summary of the privacy impact assessment publicly available in a place that is easily
28 accessible and available to the Attorney General on request. The privacy impact
29 assessment must:

30 A. Be reasonable and appropriate in scope given:

31 (1) The nature of the covered data collected, processed and transferred by the
32 covered entity;

33 (2) The volume of the covered data collected, processed and transferred by the
34 covered entity; and

35 (3) The potential risks posed to the privacy of individuals by the collecting,
36 processing and transfer of covered data by the covered entity;

37 B. Be in written form and maintained by the covered entity unless rendered out of date
38 by a subsequent assessment;

39 C. Include additional information required by the Attorney General; and

40 D. If the covered entity is a large data holder, be approved by the privacy protection
41 officer.

1 **§9618. Service providers**

2 **1. Contract.** A service provider shall follow the instructions of a covered entity and
3 may only collect, process and transfer service provider data to the extent necessary and
4 proportionate to provide a service requested by the covered entity, as set out in the contract
5 between the covered entity and the service provider. A service provider is not required to
6 collect, process or transfer covered data if the service provider would not otherwise do so.
7 A person may only act as a service provider pursuant to a written contract between the
8 covered entity and the service provider, or a written contract between one service provider
9 and a second service provider if the contract:

10 A. Clearly sets forth:

11 (1) The data processing procedures of the service provider with respect to
12 collection, processing or transfer performed on behalf of the covered entity or
13 service provider;

14 (2) Instructions for collecting, processing or transferring data;

15 (3) The nature and purpose of collecting, processing or transferring data;

16 (4) The type of data subject to collecting, processing or transferring;

17 (5) The duration of processing; and

18 (6) The rights and obligations of both parties, including a method by which the
19 service provider shall notify the covered entity of material changes to its privacy
20 practices;

21 B. Does not relieve a covered entity or a service provider of a requirement or liability
22 imposed on a covered entity or service provider under this chapter; and

23 C. Prohibits:

24 (1) Collecting, processing or transferring covered data in contravention to the
25 requirements set forth under paragraph A; and

26 (2) Combining service provider data with covered data which the service provider
27 receives from or on behalf of another person or collects from the interaction of the
28 service provider with an individual, provided that the combining is not necessary
29 to achieve a purpose described in subsection 9604, subsection 2 and is otherwise
30 permitted under a required contract.

31 A service provider shall retain copies of previous contracts entered into in compliance with
32 this subsection with each covered entity to which it provides requested products or services.

33 **2. Prohibition on certain actions.** A service provider may not collect, process or
34 transfer service provider data if the service provider has actual knowledge that a covered
35 entity violated this chapter with respect to that data.

36 **3. Assisting covered entity.** A service provider shall assist a covered entity in
37 responding to a request made by an individual regarding service provider data, by either:

38 A. Providing appropriate technical and organizational measures, taking into account
39 the nature of the processing and the information reasonably available to the service
40 provider, for the covered entity to comply with the request for service provider data; or

1 B. Fulfilling a request by a covered entity by either complying with the request
2 pursuant to the covered entity's instructions or providing written verification to the
3 covered entity that:

4 (1) The service provider does not hold covered data related to the request;

5 (2) Complying with the request would be inconsistent with its legal obligations;
6 or

7 (3) The request falls within an exception to section 9611.

8 **4. Engagement of other service providers.** A service provider may engage another
9 service provider for purposes of processing service provider data on behalf of a covered
10 entity only after providing that covered entity with notice and pursuant to a written contract
11 that requires the other service provider to satisfy the obligations of the original service
12 provider with respect to the service provider data, including that the other service provider
13 be treated as a service provider under this chapter.

14 **5. Compliance information.** In response to a reasonable request by a covered entity,
15 a service provider shall make available to the covered entity information necessary to
16 demonstrate the compliance of the service provider with the requirements of this chapter,
17 including a report of an independent assessment arranged by the service provider on terms
18 agreed to by the service provider and the covered entity, provide information necessary to
19 enable the covered entity to conduct and document a privacy impact assessment required
20 under this chapter and make available the algorithmic design evaluation required under
21 section 9615.

22 **6. Deletion or return of covered data.** At the covered entity's direction, a service
23 provider shall delete or return all covered data to the covered entity at the end of the
24 provision of services, unless retention of the covered data is required by law.

25 **7. Safeguards.** A service provider shall develop, implement and maintain reasonable
26 administrative, technical and physical safeguards that are designed to protect the security
27 and confidentiality of covered data the service provider processes consistent with section
28 9616.

29 **8. Assessments.** A service provider shall allow and cooperate with reasonable
30 assessments by the covered entity or the covered entity's designated assessor. The service
31 provider may arrange for a qualified and independent assessor to conduct an assessment of
32 the service provider's policies and technical and organizational measures in support of the
33 obligations under this chapter using an appropriate and accepted control standard or
34 framework and assessment procedure for the assessments. The service provider shall
35 provide a report of the assessment to the covered entity on request.

36 **9. Service provider relationship determination.** Determining whether a person is
37 acting as a covered entity or service provider with respect to a specific processing of
38 covered data is a fact-based determination that depends upon the context in which that data
39 is processed. A person that is not limited in the person's processing of covered data
40 pursuant to the instructions of a covered entity, or that fails to adhere to those instructions,
41 is a covered entity and not a service provider with respect to a specific processing of
42 covered data. A service provider that continues to adhere to the instructions of a covered
43 entity with respect to a specific processing of covered data remains a service provider. If
44 a service provider begins, alone or jointly with others, determining the purposes and means

1 of the processing of covered data, it is a covered entity and not a service provider with
2 respect to the processing of that data.

3 **10. Liability.** A covered entity that transfers covered data to a service provider or a
4 service provider that transfers covered data to a covered entity or another service provider,
5 in compliance with the requirements of this chapter, is not liable for a violation of this
6 chapter by the service provider or covered entity to which the covered data was transferred,
7 if at the time of transferring the covered data, the covered entity or service provider did not
8 have knowledge that the service provider or covered entity would violate this chapter. A
9 covered entity or service provider that receives covered data in compliance with the
10 requirements of this chapter is not in violation of this Act as a result of a violation by a
11 covered entity or service provider from which that data was received.

12 **11. Due diligence required.** A covered entity or service provider shall exercise
13 reasonable due diligence in selecting a service provider.

14 **12. Service provided to government entities.** Solely for the purposes of this section,
15 the requirements for service providers to contract with, assist and follow the instructions of
16 covered entities must include requirements to contract with, assist and follow the
17 instructions of a government entity if the service provider is providing a service to a
18 government entity.

19 **§9619. Third parties**

20 **1. Processing.** A 3rd party may not process 3rd-party data for a processing purpose
21 other than, in the case of sensitive data and covered data, the processing purpose for which
22 the individual gave affirmative consent or to effect a purpose enumerated in section 9604,
23 subsection 2, paragraph A, C or E and, in the case of nonsensitive data, the processing
24 purpose for which the covered entity made a disclosure pursuant to section 9608, subsection
25 1, paragraph D. A 3rd party may reasonably rely on representations made by the covered
26 entity that transferred the 3rd-party data if the 3rd party conducts reasonable due diligence
27 on the representations of the covered entity and finds those representations to be credible.

28 **2. Contract required.** A covered entity that transfers covered data to a 3rd party shall
29 enter into a written contract with the 3rd party that:

30 A. Identifies the specific purposes for which the covered data is being made available
31 to the 3rd party;

32 B. Specifies that the covered entity is transferring the covered data to the 3rd party
33 solely for the specific purposes set forth in the contract and that the 3rd party may only
34 use the covered data for those specific purposes; and

35 C. Requires the 3rd party to comply with all applicable provisions of and rules adopted
36 under this chapter with respect to the covered data that the covered entity transfers to
37 the 3rd party and to provide the same level of privacy and security protection for the
38 covered data as required by covered entities under this chapter.

39 **3. Due diligence required.** A covered entity or service provider shall exercise
40 reasonable due diligence in deciding to transfer covered data to a 3rd party.

41 **§9620. Enforcement**

1 **1. By government official.** The Attorney General, a district attorney or a counsel for
2 a municipality may bring a civil action in the name of the State or on behalf of the residents
3 of the State against a covered entity or service provider that violates this chapter to:

4 A. Enjoin the act or practice that is in violation of this chapter;

5 B. Enforce compliance with this chapter or a rule adopted under this chapter;

6 C. Obtain damages, civil penalties, restitution or other compensation on behalf of the
7 residents of the State; or

8 D. Obtain reasonable attorney's fees and other litigation costs reasonably incurred.

9 **2. By individual.** A violation of this chapter or a rule adopted under this chapter with
10 respect to the covered data of an individual constitutes an injury to that individual. The
11 injured individual may bring a civil action against the party that commits the violation,
12 except that an individual may not bring a civil action against a small business. In a civil
13 action brought under this subsection in which a plaintiff prevails, the court may award the
14 plaintiff:

15 A. Damages in an amount not less than \$5,000 per individual per violation, as adjusted
16 annually to reflect an increase in the Consumer Price Index, or actual damages,
17 whichever is greater;

18 B. Punitive damages;

19 C. Injunctive relief;

20 D. Declaratory relief; and

21 E. Reasonable attorney's fees and litigation costs.

22 **3. Arbitration agreement or waiver.** Notwithstanding any provision of law to the
23 contrary, no predispute arbitration agreement or predispute joint-action waiver is valid or
24 enforceable with respect to a dispute arising under this chapter. A determination as to
25 whether this subsection applies to a dispute must be made by a court, rather than an
26 arbitrator, without regard to whether an applicable agreement purports to delegate that
27 determination to an arbitrator. For purposes of this subsection, "predispute arbitration
28 agreement" means an agreement to arbitrate a dispute that has not arisen at the time of the
29 making of the agreement and "predispute joint-action waiver" means an agreement that
30 would prohibit a party from participating in a joint, class or collective action in a judicial,
31 arbitral, administrative or other forum, concerning a dispute that has not yet arisen at the
32 time of the making of the agreement.

33 **Sec. 2. Deadlines for certain actions.** The first algorithm assessment or design
34 evaluation required by the Maine Revised Statutes, Title 10, section 9615 is required to be
35 completed not later than the 2nd anniversary of the effective date of this Act. The first
36 certification required by Title 10, section 9612, subsection 2 and the first privacy impact
37 assessment required by Title 10, section 9617, subsection 4 are required to be completed
38 not later than the first anniversary of the effective date of this Act.

39 **Sec. 3. Effective date.** This Act takes effect 180 days after the adjournment of the
40 First Special Session of the 131st Legislature.

1 **SUMMARY**

2 This bill enacts the Data Privacy and Protection Act, which:

3 1. Governs the collection, processing and transfer of certain personal data, including
4 imposing requirements for consent to use the data, the use of personal data in targeted
5 advertising and the use of the personal data of minors;

6 2. Requires policies, practices and procedures for data privacy; and

7 3. Prohibits retaliation for the exercise of a right relating to personal data and prohibits
8 discriminatory practices in the collection, processing or transfer of personal data.