State Data Privacy and Protection Act
Section by Section Summary

Section 1. Short Title

The title of the Act will be the "[State] Data Privacy and Protection Act."

Section 2. Definitions.

The Act defines "covered entity" to include any entity that collects, processes, or transfers covered data.

"Covered data" is defined as information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. This includes derived data and unique identifiers, but does not include de-identified data, some forms of employee data, or publicly available information (each of which is separately defined).

"Sensitive covered data" is subject to heightened protections and includes:

- Social Security Numbers and other government-issued identifiers;
- past, present, and future health, diagnosis, disability, or treatment information;
- financial account, debit card, and credit card numbers along with any access code, password, or credentials;
- biometric information;
- genetic information;
- past or present precise geolocation information;
- private communications such as voicemail, email, text or information identifying parties to communications;
- any account or device log-in credentials;
- information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectations regarding collection, processing, or disclosure;
- calendar, address book, phone, text, photos, audio and video recordings maintained for private use on a device;
- photos or videos of naked or undergarment-clad private areas;
- information revealing individuals access to or viewing of TV, cable, or streaming media services;

- any information related to individuals under 17 years of age;
- an individual's race, color, ethnicity, religion, or union membership; and
- information revealing online activities over time and across third party online services

Any other covered data collected, processed, or transferred for the purpose of identifying sensitive covered data is also considered sensitive. The Attorney General is granted rulemaking authority to include additional categories of covered data within the sensitive covered data definition where those categories require similar protection as a result of new methods for collecting or processing covered data.

"Biometric information," "genetic information," and "precise geolocation information" are each specifically defined.

"Data Brokers," "large data holders," "service providers," "third parties," and "small businesses" are all defined subsets of covered entities. "Large Data Holders" are covered entities with gross revenues above $250 million and that collected, processed, or transferred covered data of over 5 million individuals/devices or the sensitive covered data of 100,000 individuals/devices in the most recent calendar year. A "small business" is a covered entity that for the prior three years earned gross annual revenues of $41 million or less, did not annually collect, process, or transfer the covered data of more than 200,000 individuals (except for processing payments and promptly deleting covered data for requested products/services), and is not a data broker.

"Collecting" means acquiring covered data by any means. "Processing" means any operation or set of operations performed on covered data. "Transferring" means to disclose, make available, or license covered data by any means or in any way. Together these terms dictate the actions of covered entities and individuals with respect to covered data.

"Targeted advertising" means displaying to an individual or device identified by a unique identifier an online advertisement that is selected based on known or predicted preferences, characteristics, or interests derived from covered data collected. It does not include responses to an individual's specific request; contextual advertising when an advertisement is displayed based on the content of a webpage or online service; or processing of data solely used for measuring or reporting advertising metrics.

Section 3. Data Minimization

The Act sets a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to either (1) provide or maintain a product or service requested by the individual, or (2) effect a purpose expressly permitted by the Act.

Permissible purposes under the Act include:

1. Completing a transaction requested by an individual;
2. Use data previously collected in accordance with the Act to:
    a. Perform system maintenance or diagnostics;
    b. Develop, maintain, repair, or enhance a product or service for which the data was collected;
    c. Conduct internal research or analytics to improve the service for which the data was collected;
    d. Perform inventory management or reasonable network management;
    e. Protect against spam; or
    f. Debug or repair errors.
3. To authenticate users;
4. To fulfill a product or service warranty;
5. To prevent, detect, protect against, or respond to a security incident;
6. To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services (meaning a violation of Federal, State, or local law punishable as a felony or misdemeanor that can directly harm);
7. To comply with a legal obligation;
8. To prevent an individual from harm where the entity believes in good faith that the individual is at risk of death, serious physical injury, or other serious health risk;
9. To effectuate a product recall;
10. To conduct a public or peer-reviewed scientific, historical, or statistical research project that is in the public interest and adheres to all relevant laws and regulations governing such research;

11. To deliver a communication that is not an advertisement, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity;
12. Messaging services;
13. To transfer assets in the context of a merger, acquisition, or similar transaction (individuals must be given opportunity to withdraw previously given consents);
14. To ensure data security;
15. To support or promote participation by individuals in civic engagement activities and democratic governance, including voting, petitioning, engaging with government proceedings, providing indigent legal aid services, and unionizing;
16. With respect to covered data previously collected in accordance with this Act, to provide advertising or marketing conducted by a first party either through direct communications with a user such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by the first party, or on a web site or app operated by the first party;
17. With respect to covered data previously collected in accordance with this Act, to provide targeted advertising.

Covered entities and service providers are prohibited from engaging in deceptive advertising or marketing of any product or service.

Section 4. Loyalty Duties.

Sets heightened protections for sensitive data collection and use (i.e., biometrics, geolocation, health data), which is only permitted when strictly necessary and not permitted for advertising purposes. Additionally, covered entities may not transfer sensitive data to a third party without affirmative express consent.

Section 5. Privacy by Design.

Covered entities have a duty to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data. These should correspond to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, and the cost of

implementation compared to the risks posed. Privacy by design must also take into account the particular privacy risks related to individuals under 17 years of age.

Section 6. Prohibition on Retaliation Against an Individual for Exercise of Rights.

Covered entities may not retaliate against an individual for exercising the rights guaranteed under the Act or for refusing to agree to the collection or processing of their data for separate products or services.

This prohibition does not prevent covered entities from differentiating the price of or levels of services based on an individual providing financial information necessarily collected and used for payment when an individual specifically requests a product. Covered entities are also not prevented from offering loyalty programs that provide discounts or rewards in exchange for continued business, provided they otherwise comply with the Act and the covered entity does not transfer that data to third parties except in enumerated limited circumstances.

Covered entities may not offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 7. Transparency.

Covered entities must provide individuals with privacy policies detailing their data collection, processing, transfer, and security activities in a readily available, understandable, and accessible manner. Any material changes to a privacy policy require covered entities to notify individuals and provide an opportunity to withdraw consent before further processing the covered data of those individuals.

Large data holders must provide short-form privacy policies.

Section 8. Individual Data Rights.

Individuals have the right to access, correct, delete, and portability of, covered data that pertains to them. The right to access includes obtaining covered data in a human-readable and downloadable format that individuals may understand without expertise, the categories of third parties and service providers their data was transferred to, the categories of sources used to collect any covered data, and the purposes for transferring the data. The rights to correct and delete covered data also require covered entities to notify other entities to whom covered data was

transferred of the corrected information or desire to have the covered data deleted. To the extent technologically feasible, individuals also have the right to export their covered data in a portable format. Covered entities are not required to comply with individual requests under this section where they are unable to verify the identity of the individual making the request.

These individual rights are subject to limited permissive exceptions for covered data use, such as complying with law enforcement or judicial proceedings. The timing for covered entities to respond to such requests depends on whether covered entities are large data holders.

Section 9. Right to Consent, Object, and Opt Out.

Individuals must be provided the means to provide and withdraw consent by the same clear, conspicuous, and easy to use means as was used to provide consent. Individuals may opt-out of the transfer of any covered data to a third party.

Covered entities engaged in targeted advertising must provide individuals with clear and conspicuous means to opt out prior to any targeted advertising and at all times afterwards.

Covered entities may not use manipulative design or dark patterns in offering the rights under this section.

Section 10. Data Protections for Children and Minors.

Covered entities are subject to additional requirements for covered data with respect to individuals under age 17. Targeted advertising is expressly prohibited if covered entities have knowledge that an individual is under 17. Knowledge is defined as:

- For high-impact social media companies (as defined), the entity knew or should have known the individual was a covered minor;
- For large data holders (as defined), that the covered entity knew or acted in willful disregard of the fact that the individual was a covered minor;
- For all other entities, actual knowledge.

Covered entities may not transfer the covered data of individuals between 13 and 17 years old to third parties without the express affirmative consent from the individual

[The Children's Online Privacy Protection Act already requires parental consent for children under 13 years of age.]

Section 11. Data Brokers.

Data brokers must place a clear and conspicuous notice on their web site and/or mobile application informing individuals they are a data broker.

Data brokers that process covered data of more than 5,000 individuals must annually register with the Attorney General. Registration includes paying a $100 fee, providing information about the data broker's activities, providing contact information, and creating a link to a website where individuals may exercise their audit rights under this Act. Data brokers face civil fines for failing to register or provide the notice required by this section.

Section 12. Civil Rights and Algorithms.

Covered entities may not collect, process, or transfer covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability. This does not prevent covered entities from diversifying an applicant, participant, or customer pool.

This section also requires covered entities that are not small businesses that use algorithms to assess their algorithms annually and submit annual algorithmic impact assessments to the Attorney General. These assessments must describe steps the entity has taken or will take to mitigate potential harms from algorithms, including any harms specifically related to individuals under 17 years of age. These assessments must also seek to mitigate algorithmic harms related to advertising for housing, education, employment, healthcare, insurance, or credit, access to or restrictions on places of public accommodation, and any disparate impact on the basis of an individual's race, color, religion, national origin, sex, or disability.

Algorithmic design evaluations must occur at the design phase of an algorithm and must cover any training data that is used to develop the algorithm.

Covered entities must make summaries of algorithmic impact assessments and design evaluations publicly available in a place that is easily accessible to individuals. (Entities may redact trade secrets.)

Section 13. Data Security and Protection of Covered Data.

Covered entities and service providers must implement and maintain data security practices and procedures that protect and secure covered data against unauthorized use and acquisition. These practices shall be appropriate to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, the current state of the art in protecting covered data, and the cost of available tools.

This section imposes specific requirements for covered entities to assess vulnerabilities, take preventive and corrective action, evaluate their systems, and retain and dispose of covered data. Covered entities must provide training to all employees with access to covered data and designate an officer or employee to maintain and implement their data security practices.

Section 14. Small Business Protections.

The section provides exemptions for small businesses. A "small business" is a covered entity that for the prior three years earned gross annual revenues of $41 million or less, did not annually collect, process, or transfer the covered data of more than 200,000 individuals (except for processing payments and promptly deleting covered data for requested products/services), and is not a data broker.

These covered entities may choose to delete, rather than correct, an individual's covered data upon receiving a verified request in section 8, are exempt from the data portability requirements under section 8(a)(4), and are fully excluded from the data security requirements in section 13(a) except for data retention obligations.

There are also exceptions for small businesses built into many sections of the Act.

Section 15. Executive Responsibility.

The CEOs (or equivalent) and privacy officers of large data holders must annually certify that their company maintains reasonable internal controls and reporting structures for compliance with the Act. This certification must be based on a review conducted by the certifying officers within 90 days of submission.

All covered entities that are not small businesses must designate one or more privacy and data security officers who must implement privacy and data security programs and ensure ongoing compliance with the Act. Large data holders must also

designate at least one of these officers as the privacy protection officer to report directly to the entity's highest official. That officer is responsible for establishing processes, conducting regular comprehensive audits, developing training and education programs for employees, maintaining records, and serving as the point of contact with enforcement authorities as related to the privacy and security requirements of the Act.

Covered entities that are not small businesses must also conduct privacy impact assessments weighing the benefits of its covered data practices against the potential consequences to individual privacy on a biennial basis and have them approved by the privacy protection officer. A summary of the privacy impact assessments must be made publicly available.

Section 16. Service Providers and Third Parties.

Service providers and third parties each have responsibilities related to covered data and may only act as a service provider or third party pursuant to a written contract. In so far as a covered entity acts as a service provider, it may only collect or process covered data for the purposes directed by the covered entity it got the data from. Service providers generally have the same responsibilities as other covered entities under the Act, with the exception that, given their non-consumer facing role, they are only required to assist the covered entities they process covered data for from fulfilling requests by individuals to exercise their rights under sections 8 of the Act.

Third parties cannot process covered data beyond the expectations of a reasonable individual. Such entities are generally subject to the same responsibilities as other covered entities under the Act.

Covered entities must conduct reasonable due diligence in selecting service providers and deciding to transfer covered data to third parties.

Section 17. Enforcement.

State Attorneys General, District Attorney, or a City Corporation Counsel may bring cases in court for injunctive relief, to obtain damages, penalties, restitution, or other compensation, and to obtain reasonable attorney's fees and other litigation costs.

Section 18. Enforcement by Persons.

Starting two years after the date the Act takes effect, persons or classes of persons may generally bring a civil action any court of competent jurisdiction seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs. This right applies to claims alleging violations of specified prohibited uses of covered data, the individual rights in sections 4, 6, 7, 8, 9, protections for children and minors against targeted advertising and the unlawful transfer of covered data in section 10, rights exercisable against registered data brokers in section 11, civil rights violations under section 12, data security protections under section 13, and rights exercisable against service providers and third parties under section 16.

No claim may be brought under this section against a small business.

Section 19. Relationship to Federal and State Laws.

Covered entities and service providers subject to and in compliance with the related data privacy and security requirements of certain specified federal laws shall be held to be in compliance with the related laws of the Act solely and exclusively to the extent that covered data is subject to the requirements in the other laws.

Section 20. Severability.

If any provision of the Act is held invalid, the remainder of the Act will remain valid to the furthest extent possible.

Section 21. Rulemaking.

The Attorney General is also granted rulemaking authority for purposes of carrying out this Act.

The Attorney General shall establish or recognize one or more acceptable privacy protective, centralized mechanisms for individuals to exercise their opt-out rights under this Act.

Section 22. Effective Date.

The Act will take effect 180 days after the date of enactment.