State Data Privacy Act
Section by Section Summary

A summary of the State Data Privacy Act by Consumer Reports and the Electronic Privacy Information Center. The entire bill draft is available in multiple formats on CR and EPIC's sites.

Section 1. Definitions

This summary covers only the most widely used definitions in the Act.

Entities covered by the Act

A **"controller"** includes any person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

A **"processor"** is any person who collects, processes, or transfers personal data on behalf of, and at the director of, a controller, another processor, or a government entity.

A **"third party"** is a person that collects personal data from another person that is not the consumer and is not a processor.

Types of data

"Personal data" is defined as any information 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 or publicly available information (each of which is separately defined).

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

- An individual's race, ethnicity, religion, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as transgender or non-binary, union membership, income level or indebtedness, or citizenship or immigration status;
- Consumer health data (as defined);
- Genetic or biometric information (as defined);
- Personal data of a consumer that a controller knows, or wilfully disregards, is a minor (defined as anyone under 18 years of age);
- Precise geolocation data;
- Social Security numbers and other government-issued identifiers;
- The online activities of a consumer (or device linked or reasonably linkable to a consumer) over time and across websites, online applications, or mobile applications that do not share common branding.

Actions by entities

“Collecting” means acquiring personal data by any means.

“Processing” means any operation or set of operations performed on personal data.

“Transferring” means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party by any means.

Together, these terms dictate the actions of controllers and individuals with respect to personal data.

Advertising definitions

“Targeted advertising” means displaying to an individual or device identified by a unique persistent identifier an online advertisement that is selected based on known or predicted preferences, characteristics, behavior, or interests associated with that individual or device. It does not include first-party advertising or contextual advertising.

“Contextual advertising” means displaying an advertisement that not vary based on the identity of the individual recipient and is based on the immediate content of a webpage on which the advertisement appears, a specific request of a consumer for information or feedback, or a consumer’s immediate presence in a geographic area with a radius no smaller than 10 miles.

“First-party advertising” means processing by a first party of its own data for the purposes of advertising that is carried out through direct communications with a consumer, in a physical location operated by the first party, or through display of an ad on the first party’s own website, app, or other online content. A “first party” is defined as a consumer-facing controller with which the consumer intends or expects to interact.

Section 2. Applicability

This Act applies to persons who conduct business in the state or produce products or services targeted to residents of the state and during the prior year (1) collected or processed the personal data of at least 35,000* consumers (except for processing payment) or (2) collected or processed the personal data of at least 10,000* consumers and derived more than 20%* of their gross revenue from the sale of personal data.

*These numbers are from state privacy laws in New Hampshire and Delaware and may be adjusted based on state population.

Section 3. Scope

This Act does not apply to Federal, State, Tribal, territorial, or local government entities.

Data that is regulated under the following federal laws is exempt from this Act: protected health information under the Health Information Portability and Accountability Act and related regulations; patient-identifying information under 42 USC 290dd-2; identifiable private information for the purposes of the protection of human subjects under 45 CFR 46; identifiable private information collected as part of human subjects research under the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; protection of human subjects under 21 CFR Parts 6, 50, and 56; personal data used or shared in research as defined in 45 CFR 164.501; information under the Health Care Quality Improvement Act of 1986; patient safety work product under the Patient Safety and Quality Improvement Act; information derived from any of the health care-related information in this subsection that is de-identified according to the Health Information Portability and Accountability Act; personal information under Title V of the Gramm-Leach-Bliley Act; personal information relevant to a consumer's credit worthiness under the Fair Credit Reporting Act; personal data under the Driver's Privacy Protection Act of 1994; personal data under the Family Educational Rights and Privacy Act; personal data under the Farm Credit Act; and personal data under the Federal Aviation Act of 1958 to the extent it preempts this Act.

This Act also exempts data collected, processed, or maintained for employment purposes, as emergency contact information, or that is necessary to administer benefits for another individual.

Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with parental consent obligations under this Act.

Section 4. Consumer Rights

Individual Rights

Individuals have the right to access, correct, and delete personal data that pertains to them. The right to access includes obtaining a list of specific third parties to which the controller has transferred personal data. To the extent technologically feasible, individuals also have the right to export their covered data in a portable format.

Controllers must respond to consumer requests within 45 days (timeline may be extended by one additional 45-day period if reasonably necessary). If a controller declines a request, the controller must provide the consumer with information about how to appeal that decision. Controllers are not required to comply with individual requests (other than opt-out requests) under this section if they cannot authenticate the request.

Right to opt-out

Individuals also have the right to opt out of the collection and processing of their personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects. Individuals may opt-out through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale.

Prohibition on use of manipulative design and dark patterns

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

Civil rights protections

Controllers and processors may not collect, process, or transfer personal data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, sex, sexual orientation, gender identity, disability, religion, ancestry, or national origin. This does not prevent covered entities from diversifying an applicant, participant, or customer pool or apply to private establishments (as defined in the U.S.C.)

Section 5. Authorized agent

A consumer may designate another person to serve as an authorized agent to exercise the rights in Section 4 of this Act. Controllers must comply with a request from an authorized agent if the controller can verify using commercially reasonable efforts the identity of the consumer and the authorized agent’s authority to act on the consumer’s behalf.

Section 6. Actions of controllers

Requirements

The act requires controllers to do the following:

1. Limit their collection, processing, and transfers of personal data to what is reasonably necessary to either provide or maintain (1) a product or service requested by the consumer, or (2) a communication, that is not an advertisement, that the consumer would reasonably anticipate in the context of the relationship between the consumer and the controller;
    a. A controller may process or transfer personal data collected under this rule (provided it is not sensitive data) to provide first-party advertising or targeted

advertising. However, the personal data cannot be used for targeted advertising if the consumer is a minor or has opted out of targeted advertising.

   b. With regard to sensitive data, the collection, processing, and transfer of such data must be strictly necessary to provide a product or service requested by the consumer.

2. Obtain affirmative consent prior to any transfer of a consumer's sensitive data;
3. Implement reasonable data security practices to protect personal data, appropriate to the volume and nature of the personal data at issue, including deleting personal data when it is no longer necessary for the purpose for which it was collected; and
4. 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 controllers to notify individuals and provide an opportunity to withdraw consent before further processing the personal data of those individuals.

Prohibitions

The act prohibits controllers from doing the following:

1. Selling sensitive data;
2. Processing personal data of a minor for the purposes of targeted advertising;
3. Retaliating against a consumer 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; and

   a. This prohibition does not prevent controllers from offering loyalty programs that provide discounts or rewards in exchange for continued business, provided they otherwise comply with the Act and the controller does not transfer that data to third parties except in enumerated limited circumstances.

4. Offering different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 7. Responsibilities of processors and controllers

Processors generally have the same responsibilities as controllers under this Act. Controllers and processors must operate under a contract. Processors must adhere to the instructions of controllers and assist controllers in meeting their obligations, particularly regarding controllers' duties to conduct data protection assessments and to respond to consumer rights requests.

Processors may only process and transfer data from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract shall also prohibit processors from combining personal data that the processor receives from a controller with personal data from other controllers or that it collects from individuals.

Section 8. Data protection assessments

Contents of data protection assessments

Controllers are required to conduct a data protection assessment for each of their processing activities that presents a heightened risk of harm to a consumer before beginning such processing. Processing that presents a heightened risk of harm includes: the collection or processing of personal data for the purpose of targeted advertising, the sale of personal data, the processing of personal data for the purpose of profiling (in certain enumerated circumstances), and the collection or processing of sensitive data.

Data protection assessments must identify the categories of personal data collected, the purposes for collecting such personal data, and whether personal data is being transferred and weigh the benefits to the controller, consumer, and the public against the potential risks to the rights of the consumer, as mitigated by safeguards that are implemented.

Reporting requirements

Controllers must submit a report of the data protection assessments to the Attorney General within 30 days and shall make a summary of the assessment publicly available. Trade secrets and confidential or proprietary information may be redacted from the report and summary. Controllers must make the full assessment available to the Attorney General upon request.

Updates and interoperability

Controllers shall review and update data protection assessments as often as appropriate considering the type, amount, and sensitivity of the personal data and the level of risk presented by the processing. A single data protection assessment may address a comparable set of processing activities, and assessments conducted to comply with another law may satisfy the requirements of this section if it is reasonably similar in scope and effect.

Section 9. De-identified data

This Section lays out the responsibilities of controllers with respect to de-identified data, including requiring that controllers take technical measures to ensure data cannot be associated with an individual, publicly commit to maintaining and using de-identified data without attempting

to re-identify the data, and contractually obligate any recipients of de-identified data to comply with these provisions. Controllers that transfer de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the de-identified data is subject and take appropriate steps to address any breaches.

Section 10. Limitations

The Act specifies that nothing in its provisions should be construed to restrict a controller or processor's ability to:

1. Comply with federal, state or municipal ordinances or regulations, except as prohibited by [state] law;
2. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities;
3. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;
4. Investigate, establish, exercise, prepare for or defend legal claims;
5. Provide a product or service specifically requested by the consumer;
6. Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
7. Take steps at the request of a consumer prior to entering into a contract;
8. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;
9. Prevent, detect, protect against or respond to security incidents relating to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the controller or processor or its services, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action;
10. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all relevant laws and regulations governing such research (with certain requirements)
11. Assist another controller, processor or third party with any of the obligations under this chapter;

12. Process personal data for reasons of public interest in the area of public health, community health or population health (with limitations)

13. Ensure the data security and integrity of personal data as required by this chapter, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;

14. Transfer assets to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller's assets (with certain requirements prior to transfer)

15. Effectuate a product recall, or to fulfill a warranty;

16. Conduct medical research in compliance with federal law; or

17. Process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data.

Nothing in this Act shall be construed to impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed by the First Amendment or under the state's journalist shield law, if applicable.

Nothing in this Act applies to any person's collection or processing of personal data in the course of such person's purely personal or household activities. For private schools, it does not require the deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such collection or processing qualifies for the exemption and that the collection and processing of personal data is reasonably necessary and proportionate to the purposes listed in this section, or, in the case of sensitive data, strictly necessary to the purposes listed in this section.

Section 11. Rulemaking

The Attorney General is granted rulemaking authority for the purpose of carrying out this Act.

Section 12. Enforcement

Enforcement by the Attorney General

The Attorney 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.

For a specified period after this Act goes into effect, the Attorney General may provide a controller that has violated this Act with an opportunity to cure the violation before bringing suit. If the Attorney General determines that a cure is possible, they may issue a notice of violation to a controller, and the controller then has 60 days to cure the violation before further action will be brought.

Enforcement by consumers

A consumer may bring a civil action against a controller or processor that violates this Act for damages of not less than $5,000 per individual per violation or actual damages, whichever is greater; punitive damages; injunctive relief; declaratory relief; and reasonable attorney's fees and litigation costs. No claim may be brought under this section against a small business.

Section 13. Severability

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

Section 14. Deadlines for certain actions

The first data protection assessments required by Section 8 are required to be completed not later than the first anniversary of the effective date of this Act.

Section 15. Effective date

This Act takes effect 180 days after enactment.