HOUSE COMMITTEE ON APPROPRIATIONS

FISCAL NOTE

HOUSE BILL NO. 1201 PRINTER'S NO. 2442 PRIME SPONSOR: Neilson

COST / (SAVINGS)

FUND	FY 2023/24	FY 2024/25
General Fund	**$0**	**$545,000**

SUMMARY:

This legislation would create the freestanding Consumer Data Privacy Act to establish consumer rights related to personal data, impose duties on data controllers and processors, and require the Attorney General to oversee compliance of the act.

ANALYSIS:

Consumers' Rights

House Bill 1201, Printer's Number 2442, creates a freestanding act, to be cited as the Consumer Data Privacy Act. This act would permit consumers to exercise the following rights regarding their personal data by a secure and reliable means, which would be managed by a business with access to and control of determining the means of processing consumer personal data (controller):

1. Confirming whether or not a controller is processing or accessing the consumer's personal data, unless the confirmation or access would require the controller to reveal a trade secret;
2. Correcting inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the consumer's personal data;
3. Deleting personal data provided by or obtained about the consumer;
4. Obtaining a copy of the consumer's personal data processed by a controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means in a manner that would disclose the controller's trade secrets; and
5. Opting out of the processing of the consumer's personal data for the purposes of targeted advertising; the sale of personal data, unless explicitly provided for under the act; or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Consumers would be permitted to designate an authorized agent to exercise the consumer's rights to opt out of the processing of their personal data on behalf of the consumer. For processing personal data of a known child, the parent or legal guardian may exercise the consumer's rights on the child's behalf. Similarly, for processing of personal data of a consumer subject to guardianship, conservatorship, or other protective arrangement, the guardian or conservator of the consumer may exercise the consumer's rights on their behalf.

Compliance of Consumers' Rights

A controller would be required to comply with a request by a consumer to exercise the consumer's right regarding their personal data as follows:

- The controller would be required to respond to the consumer no later than 45 days after receipt of

a request, and a controller would be permitted to extend the response period by an additional 45 days if it is reasonably necessary so long as they inform the consumer of the reason for the extension within the initial response period;

- The controller would be required to inform the consumer no later than 45 days after receipt of request if they decline to take action regarding the consumer's request, as well as provide the justification for why they declined to take action and instructions for how to appeal the decision;
- Any information provided in response to consumer requests would be provided by the controller, free of charge, once per consumer during a 12-month period. The controller would be permitted to charge a consumer a reasonable fee if the controller can demonstrate that their request is manifestly unfounded, excessive, or repetitive;
- A controller would not be required to comply with a consumer request to exercise rights 1-4 if the controller is unable to authenticate a request to exercise any of those rights until the consumer provides additional information reasonably necessary to authenticate the consumer and their request. A controller would not be required to authenticate right 5, but the controller would be permitted to deny an opt-out request if the controller has a good faith, reasonable, and documented belief that the request is fraudulent. The controller would need to notify the individual who made the request of such belief; and
- A controller that obtains personal data about a consumer from a source other than the consumer would be deemed in compliance with a consumer's request to delete the personal data in accordance with their rights by either retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose in accordance with the provisions of the act, or opting the consumer out of the processing of the data for any purpose except for those explicitly exempted by the act.

Duties, Responsibilities, and Authorizations of Controllers and Data Processors

The legislation imposes several duties and responsibilities upon controllers, including, but not limited to, limiting the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed and refraining from processing personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed unless otherwise provided for by the legislation. Controllers would also be required to provide a consumer with a reasonably accessible, clear, and meaningful privacy notice that includes information as explicitly enumerated by the legislation. In addition, a controller that sells personal data to a third party or processes personal data for targeted advertising would be required to clearly and conspicuously disclose the sale or processing and the manner in which a consumer may exercise the right to opt out of the sale or processing of their personal data.

Moreover, the legislation imposes duties and responsibilities on data processors, including requirements to adhere to the instructions of a controller and assist the controller in complying with their duties as imposed by the legislation. The legislation further establishes provisions relating to contracts between controllers and data processors and guidelines for determining which individuals are acting as a controller versus a data processor.

Controllers would be permitted to process personal data to the extent that the processing is reasonably necessary and proportionate to the purposes specified in the legislation and is adequate, relevant, and limited to what is necessary. A controller or processor that collects, uses, or retains personal data shall, when applicable, consider the nature and purpose of the collection, use, and retention of the personal data. Additionally, personal data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and reduce reasonably foreseeable risks of harm to a consumer. If a controller processes personal data in accordance with an exemption permitted under the legislation, the controller would be responsible for demonstrating that the processing qualifies for the exemption.

Data Protection Assessments

A controller would be required to conduct and document a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer. In the data protection assessment, a controller would need to identify and weigh the benefits that may flow, directly or indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the consumer's rights to personal data privacy, as mitigated by safeguards that can be employed by the controller to reduce the risks. These data protection assessment requirements would apply to processing activities created or generated after July 1, 2024, and would not apply retroactively.

The Attorney General would be permitted to require a controller to disclose and make available a data protection assessment that is relevant to an investigation conducted by the Attorney General. Data protection assessments would remain confidential and exempt from disclosure requirements under 5 U.S.C § 552 and Act 3 of 2008, known as the Right-to-Know Law. Disclosure of a data protection assessment to the Attorney General would also not constitute a waiver of privilege or protection in the event that information contained in the assessment is subject to attorney-client privilege.

Appeals

A controller would be required to establish a process for a consumer to appeal the controller's refusal to take action on a request by a consumer to exercise their rights within a reasonable period of time after receipt of the controller's decision to decline a request. The appeal process would be required to be conspicuously available and similar to the process for submitting a request to initiate an action to exercise a consumer's rights.

The controller would be required to inform the consumer in writing of an action taken or not taken in response to the appeal within 60 days of receipt of the appeal. If the appeal is denied, the controller would need to provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

Enforcement by the Attorney General

The Attorney General would have exclusive authority to enforce the provisions of the act. During the period beginning July 1, 2024, and ending December 31, 2025, the Attorney General shall, prior to initiating an action for a violation of this act, issue a notice of the violation to the controller or processor if the Attorney General determines that a cure is possible. The right to cure would apply for 60 days. If the controller fails to cure the violation, the Attorney General may initiate an action permitted by the act.

Beginning January 1, 2026, the Attorney General would be permitted to consider the following factors in determining whether to grant a controller or processor the opportunity to cure an alleged violation:

- The number of violations;
- The size and complexity of the controller or processor;
- The nature and extent of processing activities of the controller or processor;
- The substantial likelihood of injury to the public;
- The safety of persons or property; and
- Whether the alleged violation was likely caused by human or technical error.

Violations of the provisions of the act would constitute "unfair methods of competition" and "unfair or deceptive acts or practices" under Act 387 of 1968, known as the Unfair Trade Practices and Consumer Protection Law, and would be enforced exclusively by the Attorney General.

The Attorney General would be required to promulgate regulations necessary to implement the provisions of the act.

Exemptions

The provisions of the act would not apply to the Commonwealth or any of its political subdivisions, a nonprofit organization, an institution of higher education, a national securities associations registered under 15 U.S.C § 780-3, a financial institution or an affiliate of a financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, or any other entity or business associate explicitly excluded in the legislation.

In addition, certain personal data is explicitly excluded from the provisions of the legislation, including, but not limited to, protected health information under HIPAA and patient-identifying information for purposes of 42 U.S.C. § 290dd-2.

The legislation would take effect in six months upon enactment.

FISCAL IMPACT:

The Office of Attorney General (OAG) anticipates needing to hire two Special Investigators and two Deputy Attorneys General as a result of the requirements imposed by the legislation to authorize and enforce the provisions of the bill. As this legislation would not take effect until six months upon enactment, there will be no fiscal impact to the Commonwealth for 2023/24. OAG estimates a cost of approximately $545,000 in 2024/25 to hire the employees needed to enforce this legislation.

PREPARED BY: Brittany Van Strien

House Appropriations Committee (D)

DATE: March 18, 2024

Estimates are calculated using the best information available. Actual costs and revenue impact incurred may vary from estimates.