

**Department of Legislative Services**  
Maryland General Assembly  
2023 Session

**FISCAL AND POLICY NOTE**  
**First Reader**

Senate Bill 844  
Finance

(Senators Kramer and West)

---

**Consumer Protection – Online Products and Services – Children’s Data**

---

This bill requires a business that offers an online product likely to be accessed by children to complete a “data protection impact assessment” of the online product. The bill establishes numerous rules, procedures, and prohibitions related to the assessments. Generally, the requirement to complete an assessment applies to an online product offered to the public on or after July 1, 2024. The Office of the Attorney General (OAG) is authorized to enforce the bill and may file a civil action in a court of competent jurisdiction against a business that violates the bill’s requirements for recovery of a civil penalty and/or injunction. A business that violates the bill’s requirements is subject to a civil penalty of up to (1) \$2,500 per affected child for each negligent violation and (2) \$7,500 per affected child for each intentional violation. Nothing in the bill may be interpreted to provide a private right of action under the bill or any other law. A data protection impact assessment is protected as confidential and must be exempt from public disclosure, including under the Maryland Public Information Act.

---

**Fiscal Summary**

**State Effect:** The bill is not anticipated to materially affect State finances or operations. OAG can likely take any enforcement actions with existing budgeted resources.

**Local Effect:** None.

**Small Business Effect:** Potential meaningful.

---

## Analysis

### Bill Summary:

#### *Definitions*

A “business” is a sole proprietorship, limited liability company, corporation, association, or other legal entity that:

- is organized or operated for the profit or financial benefit of its shareholders or other owners;
- collects consumers’ personal information, or on the behalf of which another collects consumers’ personal information;
- alone, or jointly with its affiliates or subsidiaries, determines the purposes and means of the processing of consumers’ personal information;
- does business in the State; and
- satisfies at least one of the following criteria: (1) has annual gross revenues of \$25.0 million or more, periodically adjusted for inflation; (2) annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices, alone or in combination with its affiliates or subsidiaries (and for the business’s commercial purposes); or (3) derives at least 50% of its annual revenues from the sale of consumers’ personal information.

“Data protection impact assessment” (or “assessment”) means a systematic survey to assess and mitigate risks to children who are reasonably likely to access the online product at issue that arise from the data management practices of the business and the provision of the online product.

“Online product” means an online service, product, or feature.

#### *Applicability*

The bill specifies entities and information to which its requirements do not apply. For example, the bill does not apply to health information and health providers (or other covered entities) already governed by specified federal regulations and laws. Certain information collected as part of a clinical trial is also not subject to the bill’s requirements.

#### *Data Protection Impact Assessment*

This bill requires a business that provides an online product likely to be accessed by children to prepare a data protection impact assessment for the online product.

The data protection impact assessment must:

- identify the purpose of the online product;
- identify how the online product uses children’s personal information;
- identify the risks of material detriment to children that arise from the data management practices of the business; and
- address, to the extent applicable, specified factors (*e.g.*, whether the design of the online product could harm children, including by exposing them to harmful or potentially harmful content on the online product, etc.).

A data protection impact assessment prepared by a business for the purpose of compliance with any other law complies with the bill if the assessment meets the bill’s requirements. A single data protection impact assessment may contain multiple similar processing operations that present similar risks, only if each relevant online product is addressed.

A business must complete a data protection impact assessment by June 30, 2024, for any online product offered to the public that is likely to be accessed by children before that date.

A business that provides an online product likely to be accessed by children may not offer the product to the public before completing a data protection impact assessment.

The bill establishes rules and procedures related to a data protection impact assessment. Among other requirements, a business completing a data protection impact assessment must:

- maintain documentation of the assessment for as long as the online product is likely to be accessed by children;
- review each assessment every two years;
- create a plan to mitigate or eliminate the risk of material detriment before the online product is made available to children; and
- provide prominent, accessible, and responsive tools to help children or their parents or guardians (if applicable) exercise their privacy rights and report concerns.

### *Prohibitions*

The bill also establishes a number of prohibitions for a business that provides an online product likely to be accessed by children. For example, the business may not:

- use the personal information of a child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child;
- profile a child by default, with limited exceptions; or
- collect, sell, share, or retain any personal information that is unnecessary to provide an online product that a child is actively and knowingly engaged with (unless the business can demonstrate a compelling reason that doing so is in the best interests of children likely to access the online product).

#### *Written Requests from the Office of the Attorney General*

Within three business days after receiving a written request from OAG, a business that provides an online product likely to be accessed by children must provide OAG with a list of all data protection impact assessments completed pursuant to the bill's requirements.

Within five business days after receiving the written request, the business must provide OAG any data protection impact assessment completed. However, to the extent that the disclosure includes information subject to attorney-client privilege or work product protection, the disclosure may not constitute a waiver of that privilege or protection.

#### *Enforcement Provisions*

Civil penalties, fees, and expenses recovered must be deposited in the general fund with the intent that they be used to fully offset costs incurred by OAG in connection with enforcing the bill.

If a business is in substantial compliance with the bill's requirements, OAG must provide written notice before filing an action authorized by the bill. Notice must identify the specific provisions of the bill that OAG alleges have been (or are being) violated.

A business may not be liable for a civil penalty for any violation for which notice is given if the business:

- cures any violation specified in the notice from OAG within 90 days;
- provides OAG with a written statement that the alleged violations have been cured; and
- takes measures to prevent future violations that OAG agrees to be sufficient.

## *Joint Ventures*

The sharing of personal information within a joint venture or partnership is subject to the bill's requirements as though the joint venture or partnership does not exist.

**Current Law:** Although the Commercial Law Article does not specifically regulate online products likely to be accessed by children, the Maryland Personal Information Protection Act imposes certain duties on a business to protect an individual's personal information. A business in possession of personal information must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, use, modification, or disclosure.

If a data breach occurs, the business must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been (or will be) misused. If the business determines that personal information likely has been (or will be) misused, the owner or licensee of the computerized data must notify an affected individual as soon as practicable, but not later than 45 days after the business discovers or is notified of the breach. For a business that only maintains personal data, the business must notify the owner or licensee of the breach as soon as practicable but not later than 10 days after the business discovers or is notified of the breach. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security.

**Small Business Effect:** The bill establishes numerous requirements for businesses that offer online products likely to be accessed by children. While the Department of Legislative Services assumes that most entities affected by the bill are likely not small businesses, any small businesses that do meet the bill's criteria as a "business" must conduct the assessments required by the bill and may incur costs to do so.

---

## **Additional Information**

**Prior Introductions:** Similar legislation has not been introduced within the last three years.

**Designated Cross File:** HB 901 (Delegates Solomon and Wilson) - Economic Matters.

**Information Source(s):** Judiciary (Administrative Office of the Courts); Department of Legislative Services

**Fiscal Note History:** First Reader - March 1, 2023  
js/jkb

---

Analysis by: Eric F. Pierce

Direct Inquiries to:  
(410) 946-5510  
(301) 970-5510