HB 430

Department of Legislative Services

Maryland General Assembly
2016 Session

FISCAL AND POLICY NOTE
Third Reader

House Bill 430 (Delegate Kaiser, *et al.*)
Ways and Means Education, Health, and Environmental Affairs

Education - Student Data Privacy Council

This bill establishes the Student Data Privacy Council. The Maryland State Department of Education (MSDE) must staff the council. By December 31, 2017, the council must report its findings and recommendations to the Governor and General Assembly, including whether the council should be made permanent.

The bill takes effect June 1, 2016, and terminates May 31, 2018.

Fiscal Summary

State Effect: MSDE can staff the council using existing resources.

Local Effect: None.

Small Business Effect: None.

Analysis

Bill Summary: The council must:

- study the development and implementation of the Student Data Privacy Act of 2015 to evaluate the impact of the Act on (1) the protection of covered information from unauthorized access, destruction, use, modification, or disclosure and (2) the implementation and maintenance of reasonable security procedures and practices to protect covered information under the Act;

- review and analyze similar laws and best practices in other states; and

- make recommendations regarding statutory and regulatory changes to the Student Data Privacy Act based on the findings of the council and repealing the termination date of the Act that established the council to allow the council to continue its evaluation of student data privacy in the State on a permanent basis.

The State Superintendent of Schools or their designee must chair the council and is responsible for the administration of the council.

Members of the council may not receive compensation but are entitled to reimbursement for expenses under the standard State travel regulations, as provided in the State budget.

Current Law/Background: The Student Data Privacy Act of 2015 (Chapter 413) requires an operator of specified websites, online services, online applications, and mobile applications designed primarily for a preK-12 public school purpose operating in accordance with a contract to (1) protect covered information from unauthorized access, destruction, use, modification, or disclosure; (2) implement and maintain reasonable security procedures and practices to protect covered information; and (3) delete covered information upon request of the public school or local school system. In addition, an operator may not knowingly (1) engage in targeted advertising based on the data collected through the website, online service, or application; (2) except in furtherance of a preK-12 school purpose, use information to make a profile about a student; (3) sell a student's information, except as provided; or (4) disclose covered information, except as detailed in the bill. Operators may use aggregated or de-identified information under certain circumstances. Chapter 413 does not apply to general audience websites, online services, online applications, or mobile applications, even if a login is created.

At the federal level, the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) govern the privacy of student data when educational institutions engage cloud service providers.

FERPA generally prohibits the disclosure by schools that receive federal education funding of personally identifiable information from a student's education records, unless the educational institution has obtained signed and dated written consent from a parent or eligible student or one of FERPA's exceptions applies.

COPPA governs operators of websites and online services that are directed to children younger than age 13 and operators of general audience websites or online services that have actual knowledge that a user is younger than age 13. Notably, the Federal Trade Commission has clarified that if an educational institution contracts with a cloud service provider that uses the students' data for advertising or marketing purposes, then COPPA is triggered.

According to the Code of Maryland Regulations, individual student records maintained by teachers or other school personnel under certain provisions are to be confidential in nature, and access to these records may be granted only for the purpose of serving legitimate and recognized educational ends. Individual student records, with the exception of records that are designated as permanent and with other exceptions provided by law, must be destroyed when they are no longer able to serve legitimate and recognized educational ends.

Educational institutions are bound by FERPA to protect the privacy of student and family information. In addition, MSDE follows guidelines specified by the Maryland Department of Information Technology's Information Security Policy.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Information Technology, Maryland State Department of Education, Department of Legislative Services

Fiscal Note History: First Reader - February 17, 2016
min/rhh

Analysis by: Caroline L. Boice

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