



## Senate Bill 504

**Position: Unfavorable**

Committee: Finance

Date: February 26, 2026

---

Founded in 1968, the Maryland Chamber of Commerce (the Chamber) is the leading voice for business in Maryland. We are a statewide coalition of more than 7,000 members and federated partners working to develop and promote strong public policy that ensures sustained economic health and growth for Maryland businesses, employees, and families.

The Maryland Chamber appreciates the intent of Senate Bill 504 (SB 504), but we are concerned the bill's language creates unintended negative consequences. Our first concern is that the controller or processor responding to valid legal process may not be in a position to determine the underlying subject matter of the request.

In many cases, the recipient of a subpoena or summons does not have visibility into whether the request is connected exclusively to immigration enforcement. To address this concern, the Maryland Chamber recommends clarifying the language so that the exception applies only where the controller or processor has actual knowledge of the request's sole immigration-related purpose. We respectfully suggest revising the provision as follows:

### **Section 14-4712.**

**(a) Nothing in this subtitle may be construed to restrict a controller's or processor's ability to:**

**(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, State, local, or other governmental authority, EXCEPT TO THE EXTENT THAT A CONTROLLER OR PROCESSOR KNOWS AN INQUIRY, AN INVESTIGATION, A SUBPOENA, OR A SUMMONS PERTAINS SOLELY TO IMMIGRATION ENFORCEMENT.**

Second, SB 504 modifies the statutory treatment of "sensitive data" and redesignates the current definition as a "sensitive attribute." Under the proposed language, sensitive data would include not only personal data that contains a sensitive attribute, but also personal data processed "for the purpose of identifying a sensitive attribute." This approach expands the scope of the statute beyond data that directly reveals a sensitive characteristic to include data based on how it is processed.

By tying the definition to the processing purpose, subsection (hh) shifts the statutory trigger from the objective nature of the data to the way processing activities are characterized. Because Maryland law imposes heightened compliance obligations when data qualifies as sensitive, this change creates uncertainty about when those obligations are triggered. As drafted, the same data

set could be treated differently depending on how a processing activity is described, rather than on whether the data actually reveals or indicates a sensitive trait. Accordingly, we recommend removing subsection (hh) and instead incorporating tailored inference language into subsection (gg). Specifically, subsection (gg) could be amended to add:

**(gg)(5) “Sensitive data” includes inferences made by a controller based on personal data, alone or in combination with other data, which are used to indicate any of the sensitive data categories identified in subsections (gg)(1) through (gg)(4).**

Third, the bill’s revision to the definition of “publicly available information” raises both constitutional and operational issues. Specifically, SB 504 would provide that information obtained from government records qualifies as publicly available only if it is processed in accordance with any restriction or term of use imposed by the governmental entity. This amendment appears intended to address concerns about how personal information contained in public records may be used after disclosure, particularly when those records include sensitive details.

Government records serve an essential role in ensuring transparency and facilitating the lawful exchange of information. Conditioning the public status of such records on downstream processing restrictions may create uncertainty about whether information retains its public character, even when lawfully obtained. Clarifying that government records lawfully accessed remain publicly available would align the statute with established constitutional principles while preserving clarity and workability within Maryland’s privacy framework.

Finally, if HB SB 504 moves forward, we respectfully request an effective date at least one year after enactment. Additional time will be necessary for companies to interpret the revised requirements, resolve implementation questions, and update compliance programs accordingly.

