Three Compliance Curve Balls to Watch Under Maryland's Comprehensive Privacy Law (MODPA)

Aaron J. Burstein, Austin J. Del Priore

October 24, 2025

While October 1, 2025—the effective date of Maryland's Online Data Privacy Act ("MODPA" or the "Act")—has come and gone, businesses still have some time to ensure their practices are compliant. By its own terms, MODPA does not apply to "any personal data processing activities before April 1, 2026," (though it requires data protection assessments for certain processing activities that occur on or after October 1, 2025) and requires the Maryland Attorney General to consider whether to provide a 60-day cure period for alleged violations until April 1, 2027. With these buffers in mind, we highlight some of the particularly challenging features of MODPA and practical ways that businesses can address them.

(1) Significant Restrictions on "Sensitive Data" Collection and Sales

In addition to adopting a broad definition of "sensitive data," MODPA (as we've noted previously), imposes particularly stringent restrictions on "sensitive data" processing. First, MODPA establishes a type of data minimization requirement, prohibiting the collection, processing, or sharing of such data unless "strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains." Second, MODPA does not permit businesses to obtain consent to sell sensitive data.

A couple of steps can help businesses to address these restrictions. First, reviewing and documenting the extent of sensitive data collection and use will help businesses assess whether they are restricting their use to what is "reasonably necessary." Data protection assessments—which MODPA and several other states require for sensitive data processing—are a logical place to document this analysis. Second, businesses that sell sensitive data should determine whether Maryland residents are present in their data so they can apply appropriate restrictions.

(2) Strict Protections for Minors Under 18

Similar to the law's treatment of sensitive data generally, MODPA does not permit businesses to obtain consent to sell personal data about consumers under the age of 18, highlighting a continued focus on children's privacy at the state level. MODPA's restriction applies to consumers that a business "knew or should have known" to be under age 18—a contrast with the willful disregard standard of several other comprehensive state privacy laws. And moreover, because MODPA's definition of "sensitive data" encompasses the data of minors under 18, any such practices are subject to the minimization and documentation requirements noted above.

For businesses that engage in targeted advertising or sell data, the Act's minors' privacy provisions raise the importance of identifying instances of data collection that could meet Maryland's combination of an under-18 age range and a constructive knowledge standard.

(3) Assessments for All Algorithms

Finally, MODPA requires businesses to conduct a data protection assessment for processing activities that "present a heightened risk of harm to a consumer." These activities include targeted advertising, personal data sales, and sensitive data processing. Although Maryland's data processing assessment requirements track other states' laws in many respects, MODPA is unusual in requiring assessments to cover "each algorithm that is used" for heightened-risk activities.

"Algorithm" is not defined in the statute, and on its face, this requirement is potentially expansive. Focusing on algorithms that directly relate to the "heightened risk" practice being assessed could help direct resources to areas that are most relevant to the assessment.

* * *

As privacy laws continue to evolve and expand through legislation (see our recent post about changes in California) and regulators establish enforcement priorities, it's important for businesses to reassess their compliance programs regularly.