BLANKROME

Privacy, Security & Data Protection

MAY 16, 2024

Maryland Passes Unique and Operationally Challenging Privacy Law

Maryland recently became the fifth state in 2024—and the 17th U.S. state overall—to pass a comprehensive data privacy law. Effective October 1, 2025, the Maryland Online Data Privacy Act ("MODPA") contains a number of unique provisions that govern the processing of sensitive and children's data, among other things. These unique provisions, combined with the broad applicability of the law, makes MODPA one of the more operationally challenging privacy laws passed in the United States to date.

SCOPE AND APPLICABILITY

MODPA applies to individuals that do business in Maryland or target services to Maryland residents and who, during the prior calendar year, either controlled or processed the personal data of at least 35,000 Maryland residents or controlled or processed the personal data of at least 10,000 Maryland residents and derived more than 20 percent of their gross revenue from the sale of personal data. The 35,000 threshold is 0.56 percent of Maryland's total population of 6.18 million and is notably lower than other state privacy laws. Most U.S. states set a threshold for processing of 100,000 state residents. Only Delaware, with a population of 990,000, has a processing threshold as low as Maryland's. The law also lacks a full exemption for non-profit institutions as well as institutions of higher education.

The relatively low threshold for compliance combined with the lack of familiar exemptions means that MODPA will likely trigger compliance obligations for a swath of institutions that haven't had to comply with many other U.S. state privacy laws.

DATA MINIMIZATION

The MODPA introduces unique data minimization provisions that differ from those found in other state privacy laws. Under these provisions, controllers are required to limit their collection of personal data to what is reasonably necessary and proportionate *to provide and maintain a product or service requested by the consumer.* This approach contrasts with other state privacy laws, and even the European Union's General Data Protection Regulation ("GDPR"), which typically focus on the specified purposes for data collection rather than the product or service. The effect of this subtle linguistic shift could be significant—depending on how it is interpreted—particularly as it relates to the usage of website tracking and analytic technologies, which may collect information about consumers that website operators don't strictly need to provide a service.

SENSITIVE PERSONAL DATA

MODPA's restrictions regarding sensitive personal data are more extensive than its counterparts in other states. The law expressly prohibits the sale of sensitive data unless such sale is necessary to provide or maintain a specific product or service requested by a consumer. There is no exception, even where consent is obtained. This differs from all other U.S. states. The term "sale" as defined by MODPA "means the exchange of personal data by a controller, a processor, or an affiliate of a controller or processor to a third party for monetary or other valuable consideration." This definition aligns with the definition of sale under the California Consumer Privacy Act ("CCPA").

The definition of "sensitive data" under the MODPA is also slightly broader than its counterparts in other states, and includes data revealing (1) racial or ethnic origin; (2) religious beliefs; (3) sex life; (4) sexual orientation; (5) status as transgender or nonbinary; (6) national origin, citizenship, or immigration status; (7) genetic or biometric data; (8) personal data collected from a child under 13 years old; (9) precise geolocation data; and (10) certain consumer health data not subject to federal law. Again, the interaction between MODPA's strict approach toward the sale of data and the complex interaction with website tracking and analytic technologies is an issue companies will need to closely analyze.

CONSUMER HEALTH DATA

MODPA continues a recent trend in state and federal regulation to restrict the processing of "consumer health data" by entities not subject to the Health Insurance Portability and Accountability Act ("HIPAA"). Similar to the Connecticut Data Privacy Act, MODPA defines "consumer health data" as "data a controller uses to identify a consumer's physical or mental status." This specifically includes data related to gender-affirming treatment or reproductive or sexual health care.

Within the MODPA framework, consumer health data is covered under the definition of sensitive data and is subject to other restrictions related to access and confidentiality. Furthermore, a company may not use a geofence to identify, track, or collect consumer health data within 1,750 feet of a mental health, reproductive, or sexual health facility.

CHILDREN

MODPA prohibits controllers from selling personal data or processing personal data of a consumer for the purposes of targeted advertising if the controller knew or *should have known* that the consumer is under the age of 18. This "should have known" standard differs in part from the "willful disregard" standard found in other state privacy laws. The law provides no guidance on what factors a company should consider when assessing the "should have known" standard, which raises some significant compliance questions for website operators used to compliance with the Children's Online Privacy Protection Rule ("COPPA") definition of minor as opposed to the higher threshold of age 18 set by MODPA. Unlike other states, such as California or Oregon, MODPA also does not contain an opt-in provision that would permit the use of an individual under the age of 18's personal data for advertising or sale purposes with express opt-in consent.

ANTI-DISCRIMINATION

The MODPA contains a unique anti-discrimination provision prohibiting controllers from collecting, processing, or transferring personal data or publicly available data that unlawfully discriminates in, or otherwise unlawfully makes unavailable, the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, or disability. Though there are limited exceptions for self-testing, diversifying applicants, and private clubs, companies must be vigilant about the risks associated with collecting, processing, or transferring data that could lead to discrimination against consumers.

NO RULE MAKING

Despite the plethora of unique compliance obligations that MODPA imposes on businesses and institutions, there is no provision for rule making under the law. This means that companies trying to understand the meaning of these new provisions may have to wait for the Maryland Attorney General to enforce the law or at least offer interpretive guidance.

ENFORCEMENT

Like the substantive provisions of the law, enforcement of MODPA charts a different path than other U.S. state laws. For example, although MODPA does not itself contain a

private right of action, the law expressly reserves the right of consumers to bring a cause of action otherwise provided by law. This differs from many other state laws that expressly state that a violation of the law may not be used as a basis for a private cause of action.

Like a number of other states, violations of MODPA are treated as unfair, abusive, or deceptive trade practices under Maryland's Consumer Protection Act, which can be enforced by the Maryland Division of Consumer Protection of the Office of the Attorney General. The MODPA contains a *discretionary* (also unique) 60-day cure period for alleged violations that sunsets on April 1, 2027.

While the MODPA is functionally similar to many of the state privacy laws passed in recent years, the law contains a number of unique provisions that increase operational and legal risk for U.S. businesses and institutions. For these entities, complying with MODPA will require careful consideration and planning.

For additional information and assistance, contact Philip N. Yannella, Sharon R. Klein, Timothy W. Dickens, Jason C. Hirsch, or another member of Blank Rome's Privacy, Security & Data Protection group.

Philip N. Yannella
215.569.5506| philip.yannella@blankrome.com

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Timothy W. Dickens
215.569.5352 | timothy.dickens@blankrome.com

Jason C. Hirsch
215.569.5445 | jason.hirsch@blankrome.com