



Privacy & Cybersecurity Update

April 2024

Maryland Poised to Enact Privacy Law; Sets New Standard for Targeted Advertising

On April 6, the Maryland Legislature sent the [Maryland Online Data Privacy Act](#) (MODPA) to Governor Wes Moore for his signature and concurrence. Once MODPA is enacted into law, Maryland will join the growing number of states that have created comprehensive data privacy laws. MODPA grants Maryland residents a broad range of data protection rights and requires covered businesses to comply with new data privacy and information security requirements. In addition, MODPA essentially prohibits targeted advertising with respect to minors under the age of 18, unless proper consent is obtained or other limited exceptions apply. This is a significant deviation from other data privacy laws, which often only require opt-in consent for targeted advertising for consumers who are 13 (or in some instances, 16) years of age or younger.

MODPA does not create a private right of action and delegates enforcement authority to the Maryland attorney general. If enacted into law, MODPA will enter into force on October 1, 2025.

Scope of Applicability

MODPA applies to organizations that conduct business in Maryland or produce products or services targeted to Maryland residents and during a calendar year control or process the personal data (i) of at least 35,000 consumers (excluding personal data processed solely to complete a payment transaction) or (ii) of at least 10,000 consumers *and* derive over 20% of gross revenue from the sale of personal data.

MODPA includes several exemptions that are standard in data privacy frameworks, including exemptions for state and local governments, organizations governed by federal

law (e.g., HIPAA, GLBA), and certain nonprofit and educational institutions.

Key Terms

MODPA primarily regulates how data “controllers” and data “processors” can collect and process a consumer’s personal and health data. The term “consumer” is defined as any Maryland resident, but excludes individuals acting in a commercial or employment context.

The term “personal data” means any information that is linked or can be reasonably linked to an identified or identifiable consumer, but does not include “de-identified data” or “publicly available information” (each of which has its own definition).

In addition, MODPA creates additional requirements when an entity processes “sensitive data,” which is defined as a subset of personal data that includes any of the following:

- Data revealing a person’s racial or ethnic origin, religious beliefs, consumer health data (see below), sex life, sexual orientation, status as transgender or nonbinary, national origin, or citizenship or immigration status
- Genetic data or biometric data (and each term is further defined in the law)
- The personal data collected from a known child
- Precise geolocation data (i.e., technology-derived data that directly identifies the specific location of a person with precision and accuracy within a radius of 1,750 feet)

The term “consumer health data” is defined as a subset of personal data that is used to identify a consumer’s physical or mental health status and includes data related to gender-

affirming care treatment and reproductive and sexual health care.

Health Data Obligations and Geofencing

Maryland's law is relatively unique compared to other state data protection laws because of its affirmative obligations concerning confidentiality and geofencing. In particular, MODPA provides that a controller may not provide an employee or a contractor access to consumer health data unless the recipient is subject to a contractual or statutory duty of confidentiality or confidentiality of such data is required as a condition of employment.

In addition, the law prohibits a controller from providing its data processors (i.e., its service providers) access to consumer health data unless they execute agreements with certain data processing clauses (see below).

The law also categorically prohibits controllers from using a geofence to establish "a virtual boundary that is within 1,750 feet of" a mental health or reproductive or sexual health facility "for the purpose of identifying, tracking, or collecting data from or sending any notification to a consumer regarding [their] consumer health data." The term "geofence" includes boundaries established or monitored through the use of GPS technology, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology or other forms of location determination technology.

Consumer Privacy Rights

As with other state privacy laws, MODPA grants consumers the rights to:

- Confirm whether a controller is processing their personal data, and if so, the right to access such personal data
- Correct inaccurate personal data, subject to certain conditions
- Require a controller to delete their personal data, unless retention is required by law
- Obtain a copy of their personal data in a "portable and, to the extent technically feasible, readily usable format that allows the consumer to easily transmit the data to another controller without hindrance," provided such personal data is processed through automatic means
- Obtain a list of categories of third parties to which a controller has disclosed their personal data or a list of categories of third parties to which the controller has disclosed any consumer's personal data if the controller does not maintain this information in a format specific to the consumer
- Opt out from a controller's processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (see more on this below)

MODPA requires controllers to establish a process for how they can receive, process, and respond to such data privacy requests, including how they are required to "authenticate" consumer requests and timelines for when such responses must be furnished to consumers. The law also requires controllers to create a framework for how consumers can appeal a controller's decision on responding to a privacy request. However, MODPA is clear that none of these rights or other opt-out rights (see below) will require a controller to "reveal a trade secret."

Selling Data

MODPA defines the "sale of personal data" as the exchange of personal data by a controller, a processor, or its affiliates, to a third party for "monetary or other valuable consideration." With respect to selling data, MODPA:

- Grants consumers the right to opt out of the processing of personal data for purposes of the sale of personal data
- Prohibits a controller from selling sensitive data
- Prohibits a controller from selling personal data related to a consumer under the age of 18 without obtaining proper consent

Importantly, MODPA has several exemptions to clarify what is *not* considered a sale of personal data, such as the disclosure of personal data to a processor for limited purposes, to an affiliate or third party for the purposes of providing a product or service affirmatively requested by the consumer, upon the direction of the consumer, and to third parties as part of corporate restructuring- or bankruptcy-related processes.

Targeted Advertising

MODPA creates a unique framework for how controllers can engage in “targeted advertising,” which is defined as “displaying advertisements to a consumer or on a device identified by a unique identifier where the advertisement is selected based on personal data obtained or inferred from that consumer’s activities over time and across nonaffiliated websites or online applications to predict that consumer’s preferences or interests” and includes common exemptions related to online marketing. Specifically, MODPA:

- Grants consumers the right to opt out of the processing of personal data for purposes of targeted advertising
- Prohibits a controller from processing personal data for targeted advertising purposes if the controller knew or should have known that the consumer was under 18 years of age, except to the extent they obtain proper consent or such processing is necessary to provide requested goods or services

This is a significant deviation from other data privacy laws, which often only require opt-in consent for targeted advertising for consumers who are 13 (or in some instances, 16) years of age or younger.

Affirmative Obligations

In addition to the privacy rights and data processing restrictions above, MODPA imposes additional obligations on data controllers. For example, a controller:

- Cannot process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed unless it obtains the consumer’s consent
- Must limit its collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by a consumer
- Must provide an effective mechanism to allow a consumer to revoke their consent for data processing that is “at least as easy” as the mechanism used for obtaining the consent
- Must honor any consent revocation as soon as possible, but not later than 30 days after receiving the request

In addition, MODPA prohibits a controller from processing personal data in violation of discrimination-related laws,

including discrimination against consumers for exercising their privacy rights, such as through pricing differences.

Information Security and Data Protection Assessments

MODPA requires controllers to “establish, implement and maintain reasonable administrative, technical, and physical security practices” to safeguard and protect “the confidentiality, integrity, and accessibility of personal data” and such measures must be appropriate to the “volume and nature” of the personal data at issue. Accordingly, MODPA supplements other Maryland laws related to [data disposal](#) and [data security](#).

Like other privacy laws, MODPA requires a controller to conduct and document data processing assessments for each of its processing activities that present a heightened risk of harm (i.e., sale of personal data, processing of sensitive data, certain types of profiling, processing for targeted advertising) to a consumer, including an assessment for each algorithm that is used. This data protection assessment must identify and “weigh the benefits that may flow directly and indirectly from the processing to the controller, the consumer, other interested parties, and the public” against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards the controller may employ to reduce such risk, and the necessity and proportionality of the processing in relation to its stated purpose. The law provides that the controller shall factor into this assessment the use of de-identified data, consumers’ reasonable expectations, the context of the processing of personal data, and the relationship between the controller and the consumer whose personal data will be processed. Pursuant to MODPA, the Maryland Consumer Protection Division may require that a controller provide it with a data protection assessment that is relevant to an investigation it is conducting.

Privacy Notices and Other Disclaimers

Controllers are required to provide consumers with “a reasonably accessible, clear, and meaningful privacy notice” that addresses:

- The categories of personal data (including sensitive data) processed by the controller
- The purpose for processing personal data

- How consumers may exercise their privacy and appellate review rights
- The categories of personal data (including sensitive data) the controller shares with third parties, if any
- The categories of third parties with which the controller shares personal data “with a level of detail that enables a consumer to understand the type of business model of, or processing conducted by each third party”
- An active email address or other online mechanism (e.g., online form) that a consumer may use to contact the controller

If a controller sells personal data to third parties or processes personal data for targeted advertising or certain types of profiling, the controller shall clearly and conspicuously disclose these activities, as well as the manner in which a consumer may exercise the right to opt out of processing.

Processor Obligations and Data Processing Agreements

MODPA also places affirmative obligations on processors, such as those related to compliance with a controller’s instructions and assistance in responding to consumer rights requests. Moreover, the law requires processors to help meet a controller’s obligations related to the security of processing personal data and providing notification of a [data breach](#) occurring within the processor’s system. MODPA also requires controllers and processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, the duration of the processing, the types of data subject to processing, parties’ rights and obligations, confidentiality duties, compliance disclosures, and subprocessing.

The law emphasizes that “[d]etermining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed” and a processor that adheres to a controller’s data processing instructions remains a processor.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Marla M. Izbicky

312.998.4253

Marla.Izbicky@ThompsonHine.com

Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight

212.908.3971

Thora.Knight@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2024 THOMPSON HINE LLP. ALL RIGHTS RESERVED.