

# STANDARD OPERATING PROCEDURES

MDOD-IT -DATA-PRIVACY-ARTICLE 1702-SOP-V1-20260701

**TOPIC:** Privacy Procedures for Prohibition of the Sale of Personal Information in contracts and dissuasion of the resale of personal record information.

## 1.0 SCOPE

### APPLIES TO:

#### Target Organizations & Personnel

All agency personnel, full-time employees, and temporary staff within the Maryland Department of Disabilities.

All contractors, vendors, processors, and third parties operating on behalf of the State.

#### System & Data Scope

This SOP applies to all information technology (IT) systems, applications, cloud networks, and physical environments that process, store, or transmit Personal Information/Personally Identifiable Information (PI/PII).

## 2.0 PURPOSE

The Standard Operating Procedures (SOP) procedures implement cybersecurity and privacy standards required by MD-STD-315 PII & Transparency Standard. [MD Code, State Government, § 10-1702]

**IMPORTANT:** Any change to this SOP must be synchronized with the MD-STD-315 PII & Transparency Standard to ensure conformance. This SOP must be reviewed at least **every three years** and updated as needed to reflect any changes to the standards.

State Gov Article 10-1702 (Formerly called HB 1222)

[https://mgaleg.maryland.gov/2026RS/Statute\\_Google/gsg/10-1702.pdf](https://mgaleg.maryland.gov/2026RS/Statute_Google/gsg/10-1702.pdf) requires Agencies to dissuade the use of public records by data brokers for sale or resharing.

HB-0264 <https://mgaleg.maryland.gov/2026RS/bills/hb/hb0264T.pdf>

### 3.0 Responsibility Assignment Matrix

Role/Title	Specific Assigned Controls
Agency Privacy Officer (APO)	PT-2.01,PT-8.01,PT-9.01
State Chief Privacy Officer (APO)	PT-2.01
Program Administration Managers	PT-2.01, PT-8.01, PT-9.01
Agency Data Owner	PT-8.01, PT-9.01
Governance Risk Compliance (GRC), Office of Security Management (OSM)	PT-8.01
Agency Data Officer (ADO)	PT-8.01, PT-9.01
Procurement Officer	PT-8.01, PT-9.01
Office of Attorney General (OAG)	PT-8.01, PT-9.01
Public Information Officer (PIO), Records Custodian (RC)/Data Steward	PT-8.01

## 4.0 Procedures

### PT-2.01: Authority to Process PII

**WHO:** The Agency Program Manager in coordination with the Agency Privacy Officer (APO).

**WHAT:** The agency-level legal authority that permits the processing of Personal Information (PI).

**WHEN:** Prior to the procurement, deployment or modification of any IT system processing PI.

**HOW:** By conducting a Privacy Threshold Analysis (PTA) to map data collection to a specific statutory mandate, obtaining individual consent before collection, and tracking authorizations in a central repository.

The Agency Program Manager will identify a specific purpose or document the statutory authority along with the data elements (in the PTA) that permits the processing of PI .

The Agency Privacy Officer (APO) will verify and formally document the agency-level authority that permits the processing of PI in the Agency Data Catalog.

The APO and Assistant Secretary/authorized signatory for the Agency unit will review and approve the completed PTA and Privacy Impact Analysis (if required). The APO will ensure that the State Chief Privacy Officer (SCPO) has access to the signed document.

Authorized agency personnel and/or contractors must ensure that PI is processed only as explicitly authorized by statutory, regulatory, grant-based, or contractual authority.

Agency personnel will adopt the policy of using or identifying a specific purpose for collecting PI and will obtain an individual's explicit consent using State-approved intake forms prior to collecting and using the PI (per Md. Code, Gen. Prov. § 4-501).

### PT-8.01: Agency Prohibition on the Sale of Personal Information (315-9)

**WHO:** The Procurement Officer in coordination with the APO and OAG

**WHAT:** Commercial data monetization bans and data classification.

**WHEN:** During contract drafting, procurement vetting, third-party risk assessments, and system logging.

**HOW:** By inserting strict data commercialization bans into contracts, running third-party risk audits, executing Attachment Y (DUA).

In accordance with MD Code, State Government, § 10-1702 and prevent the commercialization of constituent data through the sale and redisclosure of personal records and geolocation data, MDE personnel will execute the following actions:

The Procurement Officer with the OAG will review all third-party agreements to disallow the sale of personal information collected by the Agency or Vendors on behalf of the State, strictly restricting authorized third parties from selling, reselling, licensing, renting, monetizing, or otherwise deriving commercial value from State-provided personal data.

The DoIT GRC or designee assigned to perform third-party risk assessments will conduct routine audits to verify that third parties do not repurpose PI for secondary, non-contracted uses, including but not limited to building commercial profiles, targeted/behavioral advertising, or training proprietary machine learning/AI models.

The Procurement Officer will ensure the execution of Attachment Y: Data Use Agreement to legally restrict third parties from redisclosing PI to any external entity unless expressly required to fulfill the contracted service, mandated by law, or authorized by the Data Subject.

Simultaneously, the Office of Security Management (OSM) will identify and classify all agency systems containing PI to maintain internal visibility.

#### PT-8.01.02: Implement Fair Information Practice Principles (FIPPs) to Protect Personal Records Made Available Pursuant to a PIA (315-9)

**WHO:** Agency Public Information Officers, Records Custodians/Data Stewards in coordination with OAG and the Agency Data Officer.

**WHAT:** Public Information Act (PIA) requests and field-level data minimization.

**WHEN:** Upon receiving external information requests and during routine records retention management.

**HOW:** By prioritizing aggregate/de-identified data, reviewing records at the field level rather than withholding whole documents, formally citing Standard 315 in redaction letters, and checking bulk request limits.

When collecting information, Agency Program Managers will implement FIPPs to ensure only the minimum amount of personal information necessary to meet a legitimate government purpose is requested, and data users will ensure personal information is shared only in line with specified purposes authorized by the Data Subject.

The Records Custodian/ Data Stewards, or designees, will ensure strict compliance with Maryland Archives retention schedule requirements and Office of Enterprise Data policies related to records retention.

To mitigate unauthorized redisclosure risks, the Records Custodian/Data Steward, Data Custodian will prioritize the sharing of fully de-identified or aggregate data whenever possible.

Program Administrator Managers must make determinations of data minimization strictly at the field level, not the record level; an entire record must not be withheld if specific identifying information can be safely removed.

The Records Custodian/Data Steward will formally document any field-level minimization in the response to the requestor, explicitly citing Standard 315 as the operational basis for the minimization.

Bulk information requests must be discouraged; if legally allowed, the Records Custodian/Data Steward will verify and confirm that only allowable personal record information is released in strict accordance with MD Code, State Government, § 10-1702.

## **ACRONYMS:**

ADO: Agency Data Officer

APO: Agency Privacy Officer

FIPPs: Fair Information Privacy Practices.

PII / PI: Personally Identifiable Information / Personal Information.

PTA: Privacy Threshold Analysis

PIA: Public Information Act

## **ATTACHMENTS / LINKS:**

Attachment-Y.-Data-Usage-Agreement

PTA Form\_Template

## **REFERENCES:**

State Gov Article 10-1702 (Formerly called HB 1222)

[https://mgaleg.maryland.gov/2026RS/Statute\\_Google/gsg/10-1702.pdf](https://mgaleg.maryland.gov/2026RS/Statute_Google/gsg/10-1702.pdf)

HB-0264 <https://mgaleg.maryland.gov/2026RS/bills/hb/hb0264T.pdf>

**DATE:** July 1, 2026

**REVISED:** Version 1