

Data Privacy Protection Procedures Report

State Government. Article §10–1702 (c)

Department of General Services

July 1, 2026

PURPOSE

Pursuant to MD Code, State Government, § 10-1702, this Standard Operating Procedures (SOP) document implements cybersecurity and privacy standards required by the MD-STD-315 PII & Transparency Standard.

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.

SCOPE

The procedures outlined in this SOP are specific to the following organizations within the State of Maryland:

Organization	Description
Maryland Department of General Services (DGS)	DGS provides professional and technical services for the design and construction of most State public improvements. For State-owned or leased facilities, DGS develops master plans. Moreover, DGS manages, operates, and maintains State government facilities; assesses all State-owned facilities; and manages their renewal funds. Using its expertise in lease negotiation, contracts, bidding, and real estate transactions, DGS supports the acquisition and disposal of any State interest in real property. For materials, supplies, and equipment used by State agencies, DGS manages centralized procurement. To State agencies, it also provides centralized inventory standards and control and records management.
And all contractors, vendors, processors, and third parties with access to personal information on behalf of the State.	Non-governmental third parties who process data on behalf of DGS and, consequently, have access to Marylanders' personal information.

ROLES & RESPONSIBILITIES

The procedures outlined in this SOP are assigned to the following individuals:

Name	Role	Responsibilities
Caterina Pangilinan	State Chief Privacy Officer (SCPO)	PT-2.01
Atif Chaudhry	Records Custodian	PT-9.01.02
Tiana Beaudouin	Audits and Compliance Officer	PT-2.01, PT-3.01, and PT-7.01
Christian Skipper	Agency Privacy Officer (APO)	PT-2.01, PT-3.01, PT-4.01, PT-5.01, PT-7.01, PT-9.01, PT-9.01.01, PT-10.01

Nishant Bhoyar	Agency Data Owner (DO), Agency Data Officer	PT-3.01
Various Office of State Procurement (OSP) staff	Procurement Contract Monitors (PCMs) and Procurement Officers (POs)	PT-3.01, PT-9.01, and PT-10.01
Nishant Bhoyar	Chief Information Officer (CIO)	PT-8.01, PT-9.01
Brandon Stoneburg	Agency Public Information Officer (PIO)	PT-9.01.01

PROCEDURES

PT-2.01: Authority to Process PII

Procedures
- The Agency Privacy Officer (APO) determines and documents the agency-level authority that permits the processing of PI in coordination with the State Chief Privacy Officer (SCPO). - Authorized users ensure that PI is processed only as explicitly authorized by statutory, regulatory, grant-based, or contractual authority. - DGS adopts the policy of using or identifying a specific purpose for collecting PI. - DGS obtains an individual's consent before collecting and using the PI.

PT-3.01: PII Processing Purposes

Procedures
- The APO identifies and documents the agency-defined purpose for processing PI. The APO describes the processing purposes in the public Privacy Notices and policies of DGS. - The Data Owner restricts the processing of PI to that which is compatible with the identified purposes. - The Data Owner monitors changes in processing and requires review and approval for changes through the agency's formal change control process and privacy risk assessment. - All DGS personnel treat PI on a "need to know" basis, bound by confidentiality obligations set forth in a Data Use Agreement (Attachment Y). - Procurement Officers ensure a new Data Use Agreement is executed as part of any contract that includes the processing of PI and, in the event that the PI elements listed in Attachment A to the Data Use Agreement change, modify the contract as soon as possible. Contract Monitors inform Procurement Officers prior to processing PI elements not listed on Attachment A. Procurement Officers ensure a modification is signed if any changes to the collection of PI are sought beyond original request.

PT-4.01: Consent

Procedures
- Use of PI is limited to the original purpose for which the Data Subject agreed or within the legitimate government purpose as stated within DGS' Privacy Notice. - The APO reviews, requests and implements State-approved tools or mechanisms to enable individuals to provide explicit consent for the processing of their PI prior to collection. - The APO implements a standardized, auditable mechanism to capture Data Subject consent prior to any permitted redisclosure beyond a legitimate government purpose.

- The APO oversees a simple process for individuals to withdraw their consent at any time, if allowable by law.

PT-5.01: Privacy Notice

Procedures
• The data requestor provides notice to individuals about the processing of PI that is available upon first interacting with DGS. DGS subsequently provides information about the DGS' privacy practices via a Privacy Notice on the DGS website. DGS communicates information about PI processing in clear, easy-to-understand, plain language.
• The APO ensures the Privacy Notice contains information required under Standard 315.
• The APO collaborates with DGS IT personnel and the OAG to ensure that the Privacy Notice addresses data protection practices used (security safeguards), including web-based protection practices.
• The APO ensures the Privacy Notice identifies contact information where individuals can ask questions about the Agency's privacy practices.

PT-6.01: System of Records Notice

Procedures
• Data Users conform with Fair Information Privacy Practices (FIPPs) by implementing transparency, purpose specification, and privacy and security safeguards.
• Data Users follow the Zero Trust Architecture (ZTA) to control access to PI where feasible.

PT-7.01: Specific Categories of PI/PII

Procedures
• The APO, in collaboration with the Audits and Compliance Officer, review systems used for collecting Social Security Numbers (SSNs) to , a) eliminate unnecessary collection, maintenance, and use of SSNs; b) prevent the denial to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN; and c) inform any individual who is asked to disclose their SSN whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is requested, and what uses will be made of it.

PT-8.01: Computer Matching Requirements

Procedures
• The APO confirms with the OAG if DGS is required by a federal agency to report to the Federal Data Integrity Board or required to report on a federal document.
• The Chief Information Officer develops and enters into a computer matching agreement before processing information for matching purposes.
• The Chief Information Officer independently verifies the information produced by the matching program.
• The APO, or their designee, provides individuals with notice and an opportunity to contest findings before taking adverse action.

PT-9.01: Agency Prohibition on the Sale of Personal Information (315-9)

• Procurement Officers, Contract Monitors, and the APO ensure agreements disallow the sale of personal information that has been collected by DGS or third-party vendors on behalf of the State, including strictly restricting third parties authorized to process PI from the sale/reselling, licensing, renting, monetizing, or otherwise deriving commercial value from State-provided personal data in conformity with MD Code, State Government, § 10-1702.
• The Audits and Compliance Officer or designee assigned to perform third-party risk assessments includes in the audit that the 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.
• Procurement Officers ensure the execution of Data Use Agreements (Attachment Y) to document restrictions on third-parties from redisclosing PI to any external entity unless expressly required to fulfill the contracted service, as explicitly mandated by law, or authorized by the Data Subject.
• The Chief Information Officer (CIO) identifies and classifies all systems containing PI.

PT-9.01.02: Implement FIPPs to Protect Personal Records Made Available Pursuant to a PIA (315-9)

• When collecting information, data requestors implement FIPPs to ensure only the minimum amount of personal information necessary to meet a legitimate government purpose is requested. Additionally, Data Users ensure personal information is used or shared in line with the specified purposes for which the Data Subject consented and provided the information.
• The Records Custodian, Agency Data Officer, or designee(s), ensures DGS compliance with Maryland State Archives records retention schedule requirements and Office of Enterprise Data policies related to records retention.
• The Records Custodian, Agency Data Officer, or designee(s), prioritizes the sharing of fully de-identified or aggregate data whenever possible to mitigate the risk of unauthorized redisclosure of PI.
• The Records Custodian, Agency Data Officer, or designee(s), makes the determination of data minimization at the field level, not the record level. An entire record should not be withheld if specific identifying information can be removed.
• In response to a requestor, the Records Custodian, Agency Data Officer, or designee(s), documents any minimization of identifying fields in the record and cite Standard 315 as the basis for the minimization.
• Bulk information requests are discouraged, but, if legally allowed, the Records Custodian, Agency Data Officer, or designee(s), will confirm that only allowable personal record information is released in accordance with MD Code, State Government, § 10-1702.

PT-10.01: Data Use Agreements & Third-Party Processors (315-11)

• Procurement Officers, Contract Monitors, and the APO include the State-approved Data Use Agreement (Attachment Y) in all third-party information technology (IT) contracts, explicitly prohibiting the sale, monetization, or use of PI for targeted marketing. They additionally enforce strict parameters to ensure that vendors only access necessary data fields, utilize encrypted data transfers, and mandate the secure destruction of PI upon contract termination.
• Procurement Officers, Contract Monitors, and the APO require third-parties to provide an updated "Authorized Sub-Processor List" upon request and immediately notify the State of any legal subpoenas or government requests for PI.
• Procurement Officers review Contractual Agreements in which PI is processed to ensure that agreements contain: ○ Purpose Limitation & Data Minimization ○ Legal Disclosure & State Notification Protocol ○ Prohibition on Data Monetization ○ Contractor requirement to notify the State of any law enforcement, judicial and/or government requests of the Contractor for Personal Information, including Sensitive Data

- Marketing & Behavioral Advertising Restrictions
- A list of Sub-Processors and defined Contractor oversight & accountability
- Data elements to be Processed pursuant to the contract