The State of Maryland

Executive Department

EXECUTIVE ORDER
01.01.2021.10

Maryland Data Privacy

WHEREAS, The people of Maryland should know how the personally identifiable information they provide to the State is used, shared, stored, and retained;

WHEREAS, State units have a responsibility to protect the privacy of personally identifiable information in State systems while facilitating appropriate data sharing and analyses; and

WHEREAS, A framework is urgently needed for the State to fulfill its commitments to properly collect, use, retain, disclose, and destroy personally identifiable information;

NOW, THEREFORE, I, LAWRENCE J. HOGAN, JR., GOVERNOR OF THE STATE OF MARYLAND, BY VIRTUE OF THE POWER VESTED IN ME BY THE CONSTITUTION AND THE LAWS OF MARYLAND, DECLARE THE FOLLOWING, EFFECTIVE IMMEDIATELY:

A. In this Order, the following words have the meanings indicated:

1. "Agency privacy officer" means an individual designated by a State unit to manage its implementation of reasonable security practices and procedures, and compliance with this Order.

2. "Personally identifiable information" means, in digital or physical form:

i. A full name, or first initial and last name, in combination with;

1) A Social Security number;

2) A driver's license number, a State identification number, or any other identification number issued by a State unit;

3) A passport number;

4) Characteristics of classifications protected under federal or State law; or

5) Biometric information including an individual's physiological or biological characteristics, including an individual's deoxyribonucleic acid, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity;

ii. But not:

1) Voter registration information;

2) Information publicly disclosed by the individual without being under duress or coercion;

3) Data rendered anonymous through the use of techniques, including obfuscation, deletion, redaction, or encryption, that make the individual no longer identifiable;

4) Protected health information; or

5) Information collected, processed, or shared for the purposes of:

a. Public health, including any information shared between the Maryland Department of Health and any unit of state or United States government as required by law;

b. Public safety;

c. State security;

d. The State Personnel Management System;

e. The State Retirement and Pension System; or

f. Investigation and prosecution of criminal offenses.

3. "Reasonable security procedures and practices" means security protections that are consistent with Department of Information Technology policies and standards.

4. "SCPO" means the State Chief Privacy Officer.

5. "State unit" means:

   i. The Department of Aging;

   ii. The Department of Agriculture;

   iii. The Department of Budget and Management;

   iv. The Department of Commerce;

   v. The Department of Disabilities;

   vi. Beginning on October 1, 2021, the Maryland Department of Emergency Management;

   vii. The Department of the Environment;

   viii. The Department of General Services;

   ix. The Maryland Department of Health;

   x. The Department of Housing and Community Development;

   xi. The Department of Human Services;

   xii. The Department of Information Technology;

   xiii. The Department of Juvenile Services;

   xiv. The Maryland Department of Labor;

   xv. The Department of Natural Resources;

   xvi. The Department of Planning;

xvii. The Department of Public Safety and Correctional Services;

xviii. The Department of State Police;

xix. The Department of Transportation;

xx. The Department of Veterans Affairs;

xxi. The Department of Secretary of State; and

xxii. Any other agency, department, board, commission, authority, or instrumentality of the State that elects to be subject to this Order.

B. State Chief Privacy Officer.

1. There is a State Chief Privacy Officer in the Office of the Governor.

2. The SCPO is appointed by, and serves at the pleasure of, the Governor.

3. The SCPO shall:

i. Provide the Governor with advice, recommendations, and consultation about data privacy;

ii. Supervise and direct efforts of State units to protect and secure personally identifiable information;

iii. Develop and manage the implementation of State information privacy policies that are:

1) Comprehensive, coordinated, and continuous; and

2) Balance the State's need for information collection and:

a. risks to the public; and

b. the costs of collection;

iv. Establish privacy requirements to be incorporated into agreements to share data.

v. Create and maintain inventories of sources of and systems containing personally identifiable information held by the State;

vi. Oversee the conduct of privacy impact assessments; and

vii. Assist State units with:

1) Identifying, matching, and merging corresponding personally identifiable information;

2) Drafting agreements and contracts for sharing, processing, storing, accessing, transmitting, or disposing of personally identifiable information;

3) Responding to audits of privacy and security of personally identifiable information;

4) Reducing:

a. duplicative requests for personally identifiable information; and

b. the amount of personally identifiable information collected and retained to only that necessary for the proper performance of the State unit's authorized functions;

5) Properly accounting for and budgeting the costs and resources needed to protect and securely dispose of personally identifiable information; and

6) Providing training to State unit employees about State information privacy policies.

C. Beginning no later than January 1, 2022, each State unit shall:

1. Employ reasonable security practices and procedures;

2. Designate an agency privacy official;

3. Comply with direction from the SCPO to protect and secure personally identifiable information;

4. Identify and document the legitimate government purpose of the State unit's collection of personally identifiable information;

5. Allow an individual to opt out of the State unit's sharing of information if the sharing is not required by law;

6. Provide to individuals:

   i. Access to their personally identifiable information that has been processed by the State unit, and methods to correct or amend it, or delete it if allowable by law;

   ii. At the time of the collection of personally identifiable information:

      1) Notice of:

         a. The collection;

         b. The purpose of the collection;

         c. Any legal authorities requiring the collection of personally identifiable information; and

         d. Whether the provision of the personally identifiable information is voluntary; and

      2) Instructions on how to receive information, which shall be provided upon request of the individual if allowable by law, about the types of:

         a. Personally identifiable information collected about the individual; and

         b. Sources from which the personally identifiable information was collected;

   iii. At or before the time of the State unit's sharing personally identifiable information, notice of the sharing, including:

      1) The nature and sources of personally identifiable information shared;

2) The purpose for which the personally identifiable information is shared and how it will be used;

3) The circumstances in which the personally identifiable information will be shared;

4) The recipients of the shared personally identifiable information;

5) The legal authorities for the sharing of the personally identifiable information; and

6) Any rights the individual may have to:

a. Review the personally identifiable information shared; or

b. Decline the State unit's sharing of personally identifiable information;

7. Prominently display on the State unit's website clear and comprehensive notice informing the public of the State unit's practices and activities regarding the use of personally identifiable information;

8. Adopt a privacy governance and risk management program; and

9. Take reasonable steps to:

i. Ensure that personally identifiable information collected is accurate, relevant, and timely; and

ii. Collect only the personally identifiable information that is relevant and necessary to address the legally authorized purpose of the collection.

D. The agency privacy officers shall meet at least monthly to provide the SCPO with advice and recommendations about State policies needed to protect the privacy of personally identifiable information.

E. On or before April 1 of each year, each State unit shall submit a report to the SCPO that includes:

1. An inventory of all information systems and applications used or maintained by the State unit;

2. A full data inventory of the State unit;

3. A list of all cloud services used by the State unit; and

4. A list of all permanent and transient vendor interconnections that are in place.

GIVEN Under My Hand and the Great Seal of the State of Maryland, in the City of Annapolis, this 29th day of July, 2021.

Lawrence J. Hogan, Jr.
Governor

ATTEST:

John C. Wobensmith
Secretary of State