

2610.02 Privacy Notice

Issued: April 21, 2019
Revised:

PURPOSE

Agencies that collect Potentially Personally Identifiable Data (hereafter PPID) about an individual shall have a privacy Notice.

APPLICATION

This procedure applies to all state of Michigan (SOM) Executive Branch Departments and Agencies who collect PPID. An Agency with access to PPID shall ensure its appropriate use as set forth in this and all SOM enterprise policies and procedures.

Adherence to this procedure does not guarantee compliance with all laws and regulations. Agencies need to be aware of privacy Notice requirements that may apply to data in their care and consult their legal counsel for advice on laws and regulations governing the data in their care and corresponding Notice requirements. Laws should be reviewed in conjunction with other applicable state and federal laws, rules, other privacy policies and procedures, as well as Agency-specific business practices, contracts, or grants.

CONTACT AGENCY

Department of Technology, Management and Budget (DTMB)
Chief Data Officer (CDO)

Telephone: 517-241-5545

Fax: 517-241-8715

SUMMARY

To the extent permitted by law and where applicable, each Agency that collects PPID is to inform employees and individuals about their applicable privacy policies, procedures, and Notices. Conversely, an Agency that does not collect PPID (or possess or control another Agency's PPID) is not required to provide a Notice.

PROCEDURES

- A privacy Notice will contain (at a minimum) a description of the information collected by the Agency; the source of that information if not from the individuals themselves; a statement regarding the purposes for the PPID collection; how the PPID will be used; types of entities to whom the PPID may be disclosed; the individual's rights and choices (if any), as well as the consequences, if any, for not providing the information; and where the information is maintained.
- Notice will be provided in a timely manner (at the time or before the time PPID is collected or as soon as practical afterwards) to an individual upon request.

Additionally, each Agency will deliver Notices to individuals as required by applicable laws, and in the appropriate accessible format. Where an Agency collects PPID from an individual, it shall place its privacy Notice on its website, if it has one.

- The Notice will include language about how PPID will be maintained, secured, and disposed of appropriately.
- The Notice, or corresponding policies and procedures, will provide an individual the means to communicate with the appropriate person about privacy activities, including the Notice, and any corresponding policies and procedures.
- Agencies will use reasonable efforts to draft a Notice using simple language.
- Agencies will review existing Notices (in any format) and create new Notices, as needed, to assure compliance with this procedure.
- The Agency will maintain a record or log of what Notices are given, when they are given, and to whom they are given; and maintain copies of all Notice forms that are distributed.
- Notices will be clearly dated, and agencies will track previous iterations of their Notice(s), policies and procedures, and documents that these changes are communicated to staff and individuals. An Agency informs individuals of a change to a previously communicated privacy Notice, for example, by posting notification on their website, by sending written Notice via postal mail, or email.

ROLES AND RESPONSIBILITIES

Agency

Agency Director (or Designee)

- Ensures SOM and internal Agency privacy policies and procedures are implemented and maintained to the extent necessary and properly enforced.

Privacy Protection Officer (also referred to as an Information Privacy Protection Officer (or Agency Specified Equivalent))

- Coordinates Agency compliance with this, and other, SOM enterprise-wide privacy policies and procedures and state and federal privacy laws.
- Coordinates and works with appropriate business staff to develop and implement applicable Agency policies and procedures.

DTMB

DTMB Chief Data Officer (or Designee)

- Serve as liaison to a Chief Data Steward and Privacy Protection Officer on privacy-compliance issues.

AUTHORIZATION

Authority

The CDO is accountable to the Enterprise Information Management Steering Committee for identifying privacy best practices. The CDO has authority, along with this procedure, under:

- Executive Order 2016-24.
- Administrative Guide to State Government 2610 Privacy Policy and 2610.01 Data Privacy Procedure.
- MCL 18.1101, *et seq.*; MCL 18.41.
- The Administrative Guide to State Government.

TERMS AND DEFINITIONS

The definition of terms is available in the Ad Guide Glossary (section 8000).
