State of Michigan
Administrative Guide to State Government

2610.04 Individual Access

Issued: April 21, 2020
Revised:

PURPOSE

To ensure agency privacy processes address an individual's access to the Potentially Personally Identifiable Data (PPID) it collects.

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 should consult their legal counsel for advice on laws, regulations, other policies and procedures, specific business practices, contracts, or grants applicable to their data.

CONTACT AGENCY

Department of Technology Management and Budget (DTMB)
Chief Data Officer (CDO)
Telephone: 517-241-5545 Fax: 517-241-8715

SUMMARY

Where an individual has the right of access to the PPID collected by an Agency, the Agency must develop a process (or utilize an existing process) that will provide individuals, upon request, with a reasonable opportunity to review, and if possible correct, their PPID. The word "reasonable" as used in this procedure means something that does not cause a significant financial, time, or resource-related burden to the Agency.

PROCEDURES

- Upon determining that an Agency may provide a right of access to individuals to review their PPID, that Agency follows a documented process to permit access by an individual to their PPID, if such access is reasonable and possible.
- The process must include the following:
    1. The individual must be able to review the accuracy and completeness of their PPID.
    2. Copies requested will be provided in a reasonable timeframe. An individual may be provided with summary information if agreed in advance that this is acceptable or as may be permitted by law. The Agency will communicate any fees associated with a request for access to the

individual, if permitted by law and/or Agency policy, when the request is made or as soon after as is practical.

3. The individual must be able to request in writing that any inaccurate PPID be corrected, amended or disputed, if reasonable and appropriate. The individual's written request must provide the reason and support for the requested correction or amendment, otherwise the requested change need not be considered. If an individual requests correction or amendment of disputed PPID, and the Agency denies such a request, they must provide the individual with a reason for the denial and an ability to challenge such denial unless a specific procedure and remedy already exists under state or federal law.
4. An Agency must have a process, and train users, to authenticate and verify the identity of an individual before granting access to or amending their PPID. That process should include the means to authenticate and identify an individual not solely based on just one identifier.
5. If an Agency is mailing PPID to an individual, that Agency must mail that information ONLY to the address of record, or in the case of an address change, to both the old and new address.

- The right to change data may require the individual to file a court action, if for example an individual decides to challenge the contents of a recorded public record or a law enforcement file.
- The right to amend data does not necessarily permit changes to a record or event that has actually occurred, such as investigative notes; even though PPID should be factual to the extent possible.
- An Agency must provide appropriate means of individual redress to ensure that individuals have a simple and effective way to have privacy concerns reviewed. An Agency must establish or rely on existing procedures to receive and respond to complaints or inquiries about their procedures relating to the collection and subsequent handling of PPID. The inquiry process should be easily accessible and simple to use. To the extent a concern or complaint is not adequately addressed, the Agency must provide the ability for the individual to escalate the matter.

ROLES AND RESPONSIBILITIES

Agency

Agency Director (or Designee)

- Ensures that the Agency implements, maintains, and enforces internal Agency privacy policies and procedures consistent with enterprise-wide SOM privacy policies.

Privacy Protection Officers (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 work with appropriate business staff to develop and implement applicable Agency policies and procedures.

DTMB

DTMB Chief Data Officer (or Designee)

- Serve as liaison to the Chief Data Stewards 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

Definition of terms available in the Admin Guide Glossary (section 8000).