

801 CMR 3.00: PRIVACY AND CONFIDENTIALITY

Section

- 3.01: General Provisions
- 3.02: Administration of Personal Data
- 3.03: Access to Personal Data
- 3.04: Objections and Administrative Appeals
- 3.05: Access by the Office of the Attorney General
- 3.06: Severability

3.01: General Provisions

(1) Scope and Purpose. Except where otherwise provided by law or judicial order, 801 CMR 3.00 shall apply to the collection, maintenance, and dissemination of personal data. Consistent with M.G.L. c. 66A, § 1, 801 CMR 3.00 shall not apply to:

- (a) Criminal offender record information as defined in M.G.L. c. 6, § 167;
- (b) Intelligence or evaluative information as defined in M.G.L. c. 6, § 167; or
- (c) Any information contained in a public record as defined in M.G.L. c. 4, § 7.

(2) Applicability. 801 CMR 3.00 is jointly promulgated by and, except where otherwise provided by law or judicial order, shall apply to the Executive Office for Administration and Finance, the Executive Office of Education, the Executive Office of Energy and Environmental Affairs, the Executive Office of Health and Human Services, the Massachusetts Department of Transportation, the Executive Office of Public Safety and Security, the Executive Office of Housing and Economic Development, the Executive Office of Labor and Workforce Development (each of which is referred to as “Executive Office” in 801 CMR 3.00, and any agencies, departments, boards, commissions, authorities and instrumentalities within each said Executive Office. 801 CMR 3.00 shall not preclude any Executive Office from promulgating its own regulations pursuant to M.G.L. c. 66A, § 3, subject to the approval of the Secretary of Administration and Finance. Any agency, as defined in M.G.L. c. 66A, § 1, not within an Executive Office shall be subject to 801 CMR 3.00, unless the agency adopts its own regulations consistent with the provisions in 801 CMR 3.00. Any agency within an Executive Office is authorized to disseminate personal data to such Executive Office, in accordance with M.G.L. c. 6A, § 5, or to the Office of the Governor in accordance with M.G.L. c. 66A, and each Executive Office and the Office of the Governor may request and access personal data held by any of their subordinate agencies, provided that such dissemination or access is consistent with the purposes of M.G.L. c. 66A and not otherwise prohibited by law. Executive Offices and agencies within such Executive Offices are authorized to provide access to personal data to the Massachusetts Information Technology Division (MassIT), without relinquishing control over such personal data, in connection with MassIT's provision of services under M.G.L. c. 7D, as such access is consistent with the purposes of M.G.L. c. 66A.

(3) Definitions. Refer to all definitions appearing in M.G.L. c. 66A, § 1.

3.02: Administration of Personal Data

(1) General Rules.

- (a) Each holder shall designate an information officer who shall serve as the responsible person for each personal data system maintained by the holder. The holder shall ensure that the requirements for preventing unauthorized access to or dissemination of personal data, as set out in M.G.L. c. 66A, are followed. A single employee may serve as the responsible person for more than one personal data system.
- (b) Each holder shall inform each of its employees having any responsibility or function involving the design, development, operation, or maintenance of a personal data system, or the use of any personal data contained therein, of the provisions of 801 CMR 3.00 and any other regulations promulgated under M.G.L. c. 66A, the safeguards of M.G.L. c. 66A pertaining to the operation of the personal data system, and the civil remedies available to individuals whose rights under M.G.L. c. 66A are allegedly violated.

3.02: continued

(c) Each holder shall not collect or maintain more personal data than is reasonably necessary for the performance of the holder's statutory functions. The holder shall permit only those employees whose duties reasonably require access to have access to personal data.

(d) Each holder shall take reasonable precautions to protect personal data from dangers of fire, identity theft, theft, flood, natural disaster, or other physical threat.

(e) Each holder shall maintain personal data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities, or benefits when such determinations are based upon such data.

(f) Holders may enter into contracts to hold personal data but no such contract shall relieve the holder of its obligations under M.G.L. c. 66A or 801 CMR 3.00. Every such contract shall include such provisions as are necessary to ensure compliance with M.G.L. c. 66A and 801 CMR 3.00.

(2) Record of Access. In the case of data held in automated personal data systems, and to the extent feasible with data held in manual personal data systems, each holder shall maintain complete and accurate records showing any access to or use of personal data by persons or organizations outside of or other than the holder. These records shall include every disclosure of personal data, including the identity of all such persons and organizations to which such access or use has been granted. To the extent maintained pursuant to 801 CMR 3.02(2), a list of the uses made of personal data, including the identity of all persons and organizations which have gained access to the data, shall be provided to the data subject upon request. Access to or use by employees and agents of the holder need not be recorded.

(3) Notice and Report to Secretary of Commonwealth. Each holder shall, upon the establishment, termination, or substantial change in character of a personal data system, file a report with the Secretary of the Commonwealth regarding each such personal data system, as required by M.G.L. c. 30, § 63 and c. 66A, § 2(e).

3.03: Access to Personal Data

Subject to 801 CMR 3.01 and 3.03, the holder shall not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulation which are consistent with the purposes of M.G.L. c. 66A, or is approved by the data subject if the data subject is entitled to access under M.G.L. c. 66A, § 2(I). The holder may adopt rules identifying the specific types of personal data applicable to that holder and a manner of dissemination that is consistent with 801 CMR 3.00. Nothing in 801 CMR 3.00 shall be construed as authorizing the holder to release information, the disclosure of which is prohibited by any statute other than M.G.L. c. 66A.

Consistent with the purposes of M.G.L. c. 66A and 801 CMR 3.00, the holder may disseminate personal data to persons other than the data subject as follows:

(a) The holder may disseminate personal data in response to compulsory legal process, provided that the procedures required by M.G.L. c. 66A, § 2(k) are followed. The holder need not provide the notice required under M.G.L. c. 66A, § 2(k), if a court orders otherwise upon a finding that notice to the data subject would probably so prejudice the administration of justice that good cause exists to delay or dispense with such notice.

(b) A holder may disseminate personal data to any federal, state, or local governmental entity for criminal or civil law enforcement purposes, provided that an authorized representative of the governmental entity has made a written request to the holder specifying the record desired and the law enforcement activity for which the record is sought, and the governmental entity agrees in writing to keep the personal data confidential to the extent permitted by law.

(c) The holder may disseminate personal data to the United States Census Bureau to aid the Bureau in connection with an official census or survey, provided that the Bureau agrees to keep the personal data confidential to the extent permitted by law.

(d) The holder may disseminate personal data as required by an order of a court of competent jurisdiction.

3.03: continued

(e) The holder may disseminate medical or psychiatric data to a physician treating a data subject upon the request of said physician, or to other persons to the extent consistent with federal or other applicable law, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data, but the data subject shall be given notice of such access upon termination of the emergency. The holder may disseminate personal data to other persons if an emergency arises that precludes the data subject's giving approval for the release of such data and dissemination is necessary for reasons related to the health or safety of the data subject, or in circumstances posing an immediate threat to public safety, provided that the scope of disclosure is limited to the extent necessary to alleviate or address the emergency. The data subject shall be given notice of such dissemination upon termination of the emergency.

3.04: Objections and Administrative Appeals

(1) Objections. A data subject, his or her attorney, parent or legal guardian, or other representative authorized in writing by the data subject may object to the accuracy, completeness, pertinence, timeliness, relevance or dissemination of personal data pertaining to the data subject, or the denial of access to such data maintained in a personal data system. Such individual may file an objection with the information officer in charge of the personal data system or another designated person within the agency. If the information officer or agency designee is unavailable, the data subject or his or her representative may make the objection to the agency head.

(2) Responsibilities of Holder Pursuant to Objections. Upon receiving a data subject's objection, the information officer or agency designee shall investigate the validity of the objection within 30 days of receipt of the objection.

(a) If the data subject or his or her representative requests that the personal data be corrected or amended, or requests any other change with respect to the personal data, and there is no disagreement concerning the change to be made, the information officer or agency designee shall cause such change to be made.

(b) If the information officer or agency designee determines that the objection lacks merit, he or she shall provide the data subject an opportunity to provide a statement reflecting the data subject's position regarding the data and shall include the statement with the personal data and with any subsequent disclosure or dissemination of the data in question.

(3) Appeal of Holder's Decision. Any data subject or representative who objects to the decision of the information officer or agency designee may appeal the matter to the agency head or a designee. The appeal shall be filed in writing within 30 days of receipt of notification of the decision by the information officer or agency designee under 801 CMR 3.04(2).

(a) If the agency head or designee agrees with the objection, he or she shall cause the requested correction, amendment, or other change to be made.

(b) If the agency head or designee determines that objection lacks merit, he or she shall provide the data subject an opportunity to provide a statement reflecting the data subject's position regarding the personal data and cause such statement to be included with the personal data and with any subsequent disclosure or dissemination of the data in question.

3.05: Access by the Office of the Attorney General

Whenever a data subject files or threatens to file a claim against an agency, or against any employee or officer of the agency concerning a matter within the scope of his or her official duties or employment, any personal data held by that agency that concerns the data subject and is relevant to the determination of issues in dispute may be provided to the Office of the Attorney General upon written request.

801 CMR: EXECUTIVE OFFICE FOR ADMINISTRATION AND FINANCE

3.06: Severability

If any provision of 801 CMR 3.00 or the application of any such provision to any person or circumstance is held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of 801 CMR 3.00 and the application of the subject provision to other persons or circumstances shall not be affected or impaired thereby.

REGULATORY AUTHORITY

801 CMR 3.00: M.G.L c. 66A, § 3.

(PAGES 35 THROUGH 40 ARE RESERVED FOR FUTURE USE.)