701 CMR 3.00: PRIVACY AND CONFIDENTIALITY

Section

3.01: Authority and Scope
3.02: Definitions
3.03: General Requirements
3.04: Access to Data by Persons Other than the Data Subject
3.05: Rights of the Data Subject
3.06: Notice to Secretary of State
3.07: Additional Policies and Procedures
3.08: Effective Date

3.01: Authority and Scope

(1) Authority. 701 CMR 3.00 is promulgated under the general authority accorded the Executive Office of Transportation and Construction under M.G.L. c. 66A; M.G.L. c. 30, § 63; and M.G.L. c. 214, § 3B; as added by the Fair Information Practices Act, St. 1975, c. 776.

(2) Scope. The provisions of 701 CMR 3.00 shall apply to the collection, maintenance, and dissemination of personal data contained in manual or computerized personal data systems. 701 CMR 3.00 shall not apply to:

(a) criminal offender record information as defined in M.G.L. c. 6, § 167;

(b) intelligence, analytical, or investigative criminal reports or criminal evaluative data maintained by a criminal justice agency as defined in St. 1976, c. 249;

(c) personal data or other data which are not contained in a personal data system.

(3) Application. 701 CMR 3.00 shall apply to the Executive Office of Transportation and Construction and any agency, board, department, commission or authority within said Executive Office as provided in M.G.L. c. 6A, § 19.

3.02: Definitions

Agency shall mean the Executive Office and any agency, board, department, commission or authority of the Commonwealth within the Executive Office as provided in M.G.L. c. 6A, § 19, including the Department of Public Works, Massachusetts Aeronautics Commission, Massachusetts Bay Transportation Authority, Massachusetts Port Authority, Massachusetts Turnpike Authority, and the Regional Transportation Authorities and Regional Transit Authorities established within the Executive Office of Transportation and Construction under M.G.L. c. 161B.

Agency Head shall mean the executive or administrative head of the agency.

Compulsory Legal Process. "Compulsory Legal Process" shall mean a summons, subpoena, warrant, or similar legal process, compliance with which may be enforced directly by fine, contempt, or other similar sanction.

Data Subject shall mean a person concerning whom personal data are held for any purpose in a personal data system.

Holder shall mean an agency which maintains one or more personal data systems, and any person or entity having a contract or agreement with such agency to hold personal data which are part of the agency's personal data system.

Personal Data shall mean any data directly concerning an individual which can be readily associated with that individual by a personal identifier, including medical, psychological, psychiatric, social, family, financial, vocational, employment history, and job performance data. Personal data shall not include data concerning the operations and functions of the agency as a whole, such as accounting and contract data, program data, or investigations and analyses of specific or general agency operations.

3.02: continued

Personal Data System shall mean a collection of manual or automated records:

(a) where most of the records in the typical individual file contain personal data; or

(b) where a substantial number of records in the typical individual file contain personal data, and where access to the files can be gained by use of a personal identifier.

Personal Identifier shall mean information used to fix an individual's identity, either by itself or when combined with other data readily accessible to the holder, including name, address, social security number, date of birth, mother's given name, mother's maiden name, or any letters of the mother's given or maiden name.

Secretary shall mean the Secretary of the Executive Office of Transportation and Construction.

3.03: General Requirements

(1) General Standard. Personal data in a personal data system shall be maintained with accuracy, completeness, timeliness, pertinence and relevance.

(2) Personal Data System Supervisor. Each agency head shall designate a personal data system supervisor to be responsible for policies and procedures concerning the privacy and confidentiality of all personal data systems maintained by the agency. The personal data system supervisor shall receive complaints and objections, answer questions, and direct operations with respect to the privacy, confidentiality, and security of personal data maintained in personal data systems. The personal data system supervisor, or an individual designated by him, shall also be immediately responsible for each personal data system and shall insure that the requirements of the Fair Information Practices Act and 701 CMR 3.00 are followed with respect to that personal data system.

(3) Personnel Training. Each holder shall insure that all personnel working with or having regular access to personal data are familiar with the provisions of M.G.L. c. 66A; M.G.L. c. 30, § 63; M.G.L. c. 214, § 3B; and 701 CMR 3.00.

(4) Physical Security. A holder shall take all reasonable precautions necessary to protect personal data in its personal data system(s) from physical damage by fire or other casualty and from theft or other unauthorized removal. Such precautions may include fire detection and sprinkling systems, alarm system, safes and locked files, window bars, passwords, keys, badges, or access logs.

3.04: Access to Data by Persons Other than the Data Subject

(1) General Requirement. Except as provided in 701 CMR 3.04(2), through 3.04(6), a holder shall not allow any organization or individual to have access to personal data contained in a personal data system, unless such access is specifically authorized in advance by the holder and by the data subject.

(2) Statutory Authorization. A holder may disseminate personal data from a personal data system without prior approval of the data subject if the release of such data is authorized by any statute or regulation, including but not limited to:

(a) the Public Records Act, M.G.L. c. 4, § 7 and c. 66, § 10;

(b) M.G.L. c. 30, § 38, requiring state agencies to furnish the state personnel administrator with certain information concerning employees of the Commonwealth;

(c) M.G.L. c. 81-87, 90, 161A, 161B; or St. 1956, c. 465 as amended; or St. 1952, c. 354 as amended; or

(d) any statute or regulation specifically cited by the person or organization seeking access to such data.

3.04: continued

(3) Public Records. A holder shall grant access to public records as defined by M.G.L. c. 4, § 7(26), upon request and without prior approval of the data subject, in accordance with the requirements of M.G.L. c. 66, § 10. The following types of personal data shall not be considered public records, and shall be disseminated only in accordance with the Fair Information Practices Act and 701 CMR 3.00;

(a) personnel files;

(b) medical files; or

(c) other personal data, the disclosure of which may constitute an invasion of privacy. Disclosure of particular personal data shall be found to constitute a possible invasion of privacy if all of the following are true:

1. the personal data are not presently of common knowledge, public record, or in the public view;
2. disclosure will more likely than not be embarrassing or offensive to the data subject; and
3. there is no legitimate public interest in the disclosure sufficient to outweigh the potentially embarrassing or offensive nature of the disclosure.

(4) Emergencies. A holder may disseminate without prior approval of the data subject medical or psychiatric data to a physician treating a data subject, upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject from giving approval for the release of such data; provided, however, that the data subject shall be given notice of such access as soon as practicable after release of the data.

(5) Compulsory Legal Process. A holder may disseminate personal data from a personal data system without prior approval of the data subject in response to compulsory legal process; provided, however, that the holder makes every possible effort to notify the data subject of such compulsory legal process in reasonable time that he may seek to have the process quashed. For purposes of 701 CMR 3.04(5), a reasonable time shall mean 72 hours prior to the deadline for response stated in the compulsory legal process; except that, if the deadline is less than 72 hours from the time that process is presented to the holder, a reasonable time shall mean any time prior to the deadline.

(6) Access by Employees of the Holder. A holder may, without prior approval of the data subject, authorize access to personal data in a personal data system by any employee of the holder whose duties legitimately require such access, and shall in consultation with the Secretary establish reasonable policies and procedures governing such access. Employees so authorized may include, but are not limited to, personnel staff, supervisors of data subjects, and agency heads or their designees. Such access may be authorized on a continuing or on a case-by-case basis, depending upon the nature of the employee's duties.

(7) Record of Outside Access. Each holder shall maintain a complete and accurate record of every access to or use of personal data in any personal data system by any organization other than the holder or any individual not employed by the holder. Such record shall include the name of the organization or individual requesting access, the date of the request, the type of data requested, the intended use of such data, and documentation that prior approval of the data subject where required by the Fair Information Practices Act and by 701 CMR 3.00 was properly obtained.

(8) Record of Access by Employees. Each holder shall maintain a complete and accurate record of every access to or use of personal data in any personal data system by any employee of the holder. In cases of regular and frequent access for routine administrative purposes, such record may be prepared in advance, stating the positions of individuals entitled to access, the general uses of such data, and the approximate frequency of access. In all other cases, such record shall state the name and position of the individual requesting access, the date of the request, the type of data requested, and the intended use of such data.

3.05: Rights of Data Subject

(1) Request by Data Subject. An agency, upon request of an individual, shall inform the individual in writing whether such agency holds, or has held within the previous 24 months, any personal data concerning him in a personal data system.

(2) Right of Access of Data Subject. A data subject or his authorized representative, except as provided in 701 CMR 3.05(4), shall have the right to inspect and copy any personal data concerning him in a personal data system, subject to reasonable policies and procedures established by the holder.

(3) Policies and Procedures Governing Access to Data. A holder may adopt reasonable policies or procedure governing access to personal data in a personal data system, consistent with M.G.L. c. 66A and with 701 CMR 3.00, which:

(a) insure that the data subject's representative is properly authorized;

(b) regulate the time and place for inspection and the manner and cost of copying; provided that the time for inspection shall not be unduly restricted and the cost of copying shall not be unreasonable; and

(c) require that data be inspected in the presence of or under the supervision of the holder.

(4) Denial of Access to Data. A holder shall deny a request by a data subject for access to personal data in a personal data system only if such access is prohibited by statute, including but not limited to M.G.L. c. 81-87, 90, 161A, or 161B; St. 1956, c. 465 as amended; or St. 1952, c. 354 as amended.

(5) Notification of Denial of Access to Data. A holder shall notify in writing an individual requesting inspection of his personal data in a personal data system of its denial of his request for access, the reasons therefore, and the right of appeal set forth herein.

(6) Right of Data Subject to Records of Access. Each data subject or his authorized representative shall have the right to inspect and copy the record, maintained pursuant to 701 CMR 3.04(7) and 3.04(8), of organizations or individuals who have obtained access to his personal data in a personal data system.

(7) Objections by Data Subjects. A data subject or his authorized representative may file an objection with a holder regarding the accuracy, completeness, relevance, use or dissemination of his personal data in a personal data system, or the denial of access to such data. During the pendency of the objection, the holder shall make all reasonable attempts not to disseminate the disputed data, or, if dissemination is necessary, to include written notification of the nature of the objection.

(8) Procedures for Objection. Objections shall be filed in writing with the personal data system supervisor or, if that person is unavailable, with the agency head or his designee, specifying the grounds for the objection and the corrective action requested. The personal data system supervisor shall notify in writing the agency head of the nature of the objection, shall note in writing the nature of the objection in the data subject's file, and shall promptly investigate the validity of the objection.

(9) Resolution of Objection. Within 30 days of the receipt of the objection, the personal data system supervisor shall notify in writing the data subject and the agency head whether or not the objection has been found to be meritorious, and of any action taken as provided below in accordance with that finding.

(a) If the personal data system supervisor approves the corrective action requested by the data subject, he shall take such action, and shall remove from the file the written notation of the nature of the objection.

(b) If the personal data system supervisor does not approve the corrective action requested, he shall prepare a written statement summarizing the data subject's claim, which shall be a permanent part of the data subject's personal data and shall be included in any subsequent disclosure or dissemination of the disputed data. The data subject shall be provided with a copy of this statement and an opportunity to have a statement reflecting his views also included in his file and disseminated with the disputed data.

3.05: continued

(10) Judicial Relief. No provision of 701 CMR 3.05 shall be interpreted in such a way as to preclude a data subject or the Attorney General from bringing an action in a court of proper jurisdiction in accordance with M.G.L. c. 214, § 3B.

(11) Statement of Rights. Upon request, a holder shall furnish to any person requested to provide personal data a statement listing all individual rights set forth in 701 CMR 3.00.

3.06: Notice to Secretary of State

Each holder shall, by September 1, 1976 and upon the subsequent establishment, termination, or substantial change in character of a personal data system, or upon other request by the Secretary of State, file a report with the Secretary of State and the Secretary regarding each personal data system it operates. Such report shall include the information required by M.G.L. c. 30, § 63, and any other information requested by the Secretary of State.

3.07: Additional Policies and Procedures

A holder may establish additional policies and procedures, consistent with the provisions of the Fair Information Practices Act and 701 CMR 3.00, to carry out the purposes of the Act, provided that any such policies or procedures which are reduced to writing shall, prior to issuance, be approved by the Secretary or his designee.

3.08: Effective Date

701 CMR 3.00 shall take effect immediately upon filing.

REGULATORY AUTHORITY

701 CMR 3.00: M.G.L. c. 66A; c. 30, § 63; c. 214, § 3B.