965 CMR 2.00: FAIR INFORMATION PRACTICES ACT

Section

2.01: General Provisions

(1) Authority. 965 CMR 2.00 is promulgated pursuant to M.G.L. c. 66A, § 3.

(2) Application. 965 CMR 2.00 shall apply to the Department of the State Auditor.

(3) Scope; Exemptions. 965 CMR 2.00 shall govern the collection, maintenance and dissemination of personal data. 965 CMR 2.00 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;

(c) Personal data contained in a public record as defined in M.G.L. c. 4, § 7;

(d) Information not otherwise excluded by 965 CMR 2.01(3)(a) through (c) that is gathered during the course of an audit conducted pursuant to M.G.L. c.11, §§ 12 and 13, until such time as the audit is released;

(e) Information not otherwise excluded by 965 CMR 2.01(3)(a) through (d) that is gathered by the Department pursuant to M.G.L. c. 75C, c. 75D, and c. 93, § 20A; and

(f) Any other statute restricting the release of personal data.

(4) Policy on Fees. Where applicable, the Department will charge fees where an individual requests a copy be made of the record to which he is granted access, pursuant to the fee schedule set forth in 965 CMR 2.01(5).

(5) Fee Schedule. The Department will charge a fee substantially equivalent to the actual cost of reproducing records and an additional fee reasonably related to the cost of making a search of a system of records.

(6) Payment of Fees. The Department will require prepayment of fees unless it waives the requirement.

2.02: Definitions

As used in 965 CMR 2.00, unless the context otherwise requires, the terms set forth below are defined as follows:

Audit Trail shall mean a record by the holder of certain persons or entities specified in 965 CMR 2.04(13) who obtain access to personal data and shall include the identity of such persons or entities gaining access and their intended use of such data.

Authorized Representative shall mean an agent expressly appointed by the data subject, including, but not limited to, an attorney at law.

Collects shall mean gathers, obtains, or receives personal data.

Data Subject shall mean an individual to whom personal data refers. This term shall refer only to human beings, and shall not include corporations, corporate trusts, partnerships, limited partnerships, trusts, other similar entities, entities subject to audit pursuant to M.G.L. c. 11, §§ 12 and 13, or schools

subject to review pursuant to M.G.L. chs. 75C, 75D, and 93, § 20A.

2.02: continued

Department of the State Auditor or Department shall mean the agency of government created by M.G.L. c. 11, § 2.

Disseminates shall mean transfers personal data, for any purpose, from a holder to any other agency, person, or entity.

Holder shall mean:

(a) The Department of the State Auditor or

(b) Any person or entity which contracts with or has an agreement with the Department whereby personal data is held as a part or as a result of performing a governmental or public function or purpose; or

(c) Any subcontractor of a holder described above who holds personal data as a part of or as a result of performing a governmental or public function or purpose.

Holds shall mean collects, stores, maintains, disseminates, or uses, whether manually, mechanically, or electronically.

Maintains shall mean stores, updates, or corrects personal data.

Personal Data shall mean any information concerning an individual which, because of a personal identifier including, but not limited to, name, identifying number, mark, or description that can be readily associated with a particular individual; provided, however, that such information is not contained in a public record as defined in M.G.L. c. 4, § 7 clause 26, and not referred to in 965 CMR 2.02.

Personal Data System shall mean a system of records containing personal data which is organized in such a way that the data is retrievable by the identity of the data subject.

Personal Identifier shall mean any element of data which may be used to determine a person's identity, either by itself or when combined with other data available to the holder. Such data may include, but is not limited to: name, address, social security number, date of birth, race, zip code, mother's given name or maiden name, or other similar device.

State Auditor shall mean Auditor of the Commonwealth or a designated member of the Department.

2.03: Information Officers

(1) Officer Designation. The State Auditor shall designate a person who shall serve as the responsible person for each personal data system the Department maintains in accordance with M.G.L. c. 66A, § 2(a). A single employee may serve as the responsible person for more than one such system.

(2) Duties and Responsibilities. The officer described in 965 CMR 2.03(1) shall with respect to the system or systems for which he is immediately responsible:

(a) Ensure that the requirements for preventing unauthorized access to personal data, as set out in M.G.L. c. 66A and in 965 CMR 2.00, are followed;

(b) Receive complaints and objections concerning the operation of the personal data system for which he is responsible and the implementation of 965 CMR 2.00; and

(c) Answer questions concerning the operation of the personal data system for which he is responsible and the implementation of 965 CMR 2.00.

2.04: Administration of Personal Data

(1) General. The holder shall not collect, maintain, or disseminate any personal data that is not essential for the performance of functions authorized by law, except where otherwise provided by statute or judicial order.

2.04: continued

(2) Holder Agreements.

(a) A holder shall not allow any other person, entity, or agency to hold personal data in the absence of an express contract or agreement.

(b) A holder which enters into a contract or agreement with any other person, entity, or agency, to hold personal data, shall:

1. expressly inform the other person, entity, or agency of its status as a holder under 965 CMR 2.00; and

2. contractually bind the other holder to its obligation under 965 CMR 2.00 and M.G.L. c. 66A.

(c) A holder shall ensure that all contracts and agreements affecting the collection, maintenance, or dissemination of personal data between it, or another holder of the same personal data, and the person or entity not otherwise subject to 965 CMR 2.00 shall contain provisions requiring compliance with 965 CMR 2.00 and M.G.L. c. 66A.

(3) Destruction of Obsolete Personal Data. Each holder shall develop and implement a definite plan for the destruction of obsolete personal data with the approval of the Records Conservation Board, pursuant to M.G.L. c. 30, § 42.

(4) Use of Personal Data for Unrelated Purposes. Except where otherwise provided by statute or judicial order, personal data collected for one purpose shall not be used for another unrelated purpose without the informed consent of the data subject.

(5) Access by a Holder. A holder shall have unlimited access, subject to 965 CMR 2.04(6), to personal data it holds, or which is held on its behalf by another holder.

(6) Access by Employees of the Holder. Each holder shall permit only those employees whose duties require access to the personal data to have access. They shall be trained in the standards of confidentiality and security required by 965 CMR 2.00.

(7) Access by Non-Holders. A holder shall not allow any person, entity, or agency, who is not employed by the holder, to have access to the personal data unless such access is:

(a) Authorized by statute or regulations consistent with the purpose of M.G.L. c. 66A and 965 CMR 2.00; or

(b) Approved by the data subject, or the data subject himself has access under statute or 965 CMR 2.00; or

(c) Demanded by another holder as authorized by 965 CMR 2.04(5); or

(d) In response to compulsory legal process. The Department will, as required by M.G.L. c. 66A, § 2(k), ensure that no personal data are made available from its personal data systems in response to a demand for data made by means of a compulsory legal process unless the data subject has been notified of such a demand in reasonable time that he may seek to have the process quashed.

(8) Access by Data Subject. Access by data subject is governed by 965 CMR 2.06.

(9) Access in Medical or Psychiatric Emergencies. Where release of personal data is not otherwise authorized by statute or regulation, a holder may disseminate 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 upon termination of the emergency.

(10) Physical Security. Each holder shall take all reasonable steps to protect the personal data from physical damage or removal, including but not limited to provisions for:

(a) Adequate fire detection and sprinkler systems;

(b) Protection against smoke and water damage;

(c) Alarm systems, safes, and locked files or other reasonably expected ways to prevent loss through larceny or other means of removal for manually held data; and

(d) Passwords, keys, access logs, or other reasonably expected ways to prevent loss through

larceny or other means of removal for mechanically or electronically held data.

2.04: continued

(11) Duplicate Files.

(a) Each holder shall ensure that the number of duplicate personal data files are held to an absolute minimum.

(b) Each holder shall ensure that any duplicate personal data files are maintained under the requirements of 965 CMR 2.00.

(12) Personnel Training. The State Auditor shall inform all of his employees who have responsibilities or functions for the design, development, operation, or maintenance of a personal data system, or the use of a personal data system therein, of the provisions of these regulations and of the civil remedies described in M.G.L. c. 214,§ .3B, available to individuals whose rights under M.G.L. c. 66A are allegedly violated, and shall use his best effort to ensure that such employees understand and comply with 965 CMR 2.00.

(13) Audit Trail Procedures. The officer in charge of each system shall maintain as an audit trail records which show any access to or use of personal data he holds; provided, however, that access by employees within the Department of the State Auditor need not be recorded. In the case of personal data systems in which personal data are stored, in whole or in part, in a computer or in electronically controlled or accessible files, the audit trail shall include a complete and accurate record of every disclosure of personal data, including the identity of all persons and organizations to whom such access or use has been granted and their declared intentions regarding the use of such personal data. In the case of all other personal data systems, the audit trail shall include such information to the maximum extent feasible. The audit trail shall be deemed part of the data to which it relates for all purposes under 965 CMR 2.00.

(14) Objection by Data Subject -- Dispensing Holding Activities. A data subject may file an objection with the holder regarding procedures for holding data, in accordance with 965 CMR 2.07. During the pendency of any objection, except where otherwise provided by law or judicial order, the holder in question shall make all reasonable attempts to dispense with any further holding activities beyond mere storage, relating to the particular data in question, until such objection has been resolved.

2.05: Enforcement

(1) Sanctions.

Employees of a Holder. Any employee of the holder found breaching the confidentiality of data subjects through the violation of 965 CMR 2.00 shall be subject to reprimand, suspension, dismissal, or other disciplinary measures by the State Auditor consistent with the Personnel Manual of the Department and may be denied future access to or contact with personal data and removed from any holding responsibilities relative to such information.

2.06: Access by Data Subjects

(1) Public Inquiry. Where an individual has reason to believe that personal data relating to him are held, the individual may request, in writing, that the State Auditor or his designee locate all personal data held by the Department of the State Auditor.

(2) Request of Individual for Notification of Holding. The Department will inform any individual in writing, within 20 days of receipt of a request, whether the Department maintains any personal data concerning such individual.

(3) Right of Data Subject to Access. Unless access by a data subject is prohibited by statute, the Department will, as promptly as possible, but in any event within 20 days of a receipt of a request, grant access to any data subject to any personal data concerning him which the Department holds. In addition, such data subject shall have the right to inspect and copy any personal data to which he has access.

(4) Notification of Denial of Access to Data. The Department will, within 20 days of a receipt of a request, notify an individual in writing, in terms comprehensible to him, of its denial of his request for

access, and the reasons therefore.

2.07: Objections and Administrative Appeals

(1) Objections by Data Subject. A data subject who objects to the collection, maintenance, dissemination, use, accuracy, completeness, type of, or denial of access to personal data held regarding him may file an objection with the officer in charge of the personal data system.

(2) Responsibilities of Holder Pursuant to Objections. Pursuant to an objection by the data subject, the officer responsible for a data system shall within 30 days of the receipt of the objection:

(a) Investigate the validity of the objection; and,

(b) If, after the investigation:

1. the objection is found to be meritorious, correct the contents of the data or the methods for holding or the use of such data; or,

2. if the objection is found to lack merit, provide the data subject the opportunity to have a statement reflecting his views recorded and disseminated with the data in question.

(c) Notify in writing the data subject of his decision.

(3) Appeal of Holder's Decision. Any data subject, or his authorized representative, who objects to the decision of the officer in charge of the personal data system, may appeal the matter to the State Auditor. The appeal shall be filed in writing within 30 days of the notification of the decision by the officer in charge of the personal data system.

(4) State Auditor -- Adjudicatory Hearing. The State Auditor or his designee hearing an appeal filed pursuant to 965 CMR 2.07(3) shall convene an adjudicatory hearing, in accordance with the provisions of M.G.L. c. 30A, within 30 days of the receipt of such an appeal, and render a decision on the merits within 30 days of the conclusion of said hearing.

(5) Judicial Relief. No provision of 965 CMR 2.07 shall be interpreted in such a way as to prevent a data subject or Attorney General from bringing action in a court of proper jurisdiction in accordance with M.G.L. c. 214, § 3B; however, procedures provided herein must be exhausted before judicial relief can be sought under M.G.L. c. 214, § 3B or any other statute.

2.08: Disclosure of Personal Data to the Attorney General

(1) Where a suit (or legal proceeding) has been threatened or instituted by a data subject against the Department of the State Auditor or against any official or employee of the Department, arising from his or her official duties or scope of employment, any personal data concerning the data subject, held by the Department that is or employs a party to such suit (or legal proceeding), which is relevant to a determination of the issues in dispute, may be furnished to the Attorney General, or authorized assistant attorney general, who may further disclose such personal data to the extent he or she deems necessary for purposes of representing the defendant(s), subject to the following conditions:

(a) Disclosure shall be furnished in response to a written or oral request from the Office of the Attorney General, which shall indicate the purpose for which the personal data is requested and describe, with particularity, the data requested; and

(b) Personal data of persons not party to the litigation (or legal proceeding) will be redacted in order to protect the privacy interests of such persons.

(2) In the event that a personal data system maintained by the Department of the State Auditor, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising under a statute or a regulation, rule, or order issued pursuant thereto, the relevant data may be referred to the Attorney General in order to enforce or implement the statute or a regulation, rule, or order issued pursuant thereto, or to investigate or prosecute such violation.

2.08: continued

(3) Nothing in 965 CMR 2.08 shall be construed to authorize the Department of the State Auditor to release information the disclosure of which is prohibited by any statute other than the Fair Information Practices Act, M.G.L. c. 66A.

REGULATORY AUTHORITY

965 CMR 2.00: M.G.L. c. 66A, § 3.