Sec. 36a-1-70. Personal data

(a) **Authority**

These Regulations are promulgated pursuant to the provisions of section 4-196 of the General Statutes.

(b) **Definitions**

(1) "Department" means the Department of Banking and includes the Banking Commissioner.

(2) "Financial institutions" includes all institutions, corporations, partnerships, organizations, associations, sole proprietorships, other individuals and enterprises regulated by the Department, and also includes applicants to become financial institutions.

(3) "Licensee or registrant" means any individual who, or personnel of any financial institution which, has been granted by the Department or has applied to the Department for a permit, certificate, approval, registration, license, charter or similar form of permission required by law.

(4) "Personal data" means any information, as set forth in Section 4-190 (9) of the General Statutes, and other data, as defined in subsection (7) of this section concerning any individual.

(5) "Category of personal data" means the classification of personal information set forth in the Personal Data Act, Section 4-190 (9) of the General Statutes.

(6) "Personnel of financial institutions" includes all organizers, directors, incorporators, officers and employees of financial institutions.

(7) "Other data" means any information which because of name, identifying number, mark or description can be readily associated with a particular person.

(c) **General Nature and Purpose of Personal Data Systems**

(1) Personnel Records.

(A) All personnel records are maintained and under the control of the Connecticut Department of Banking, which is located at 260 Constitution Plaza, Hartford, Connecticut.

(B) Personnel records are maintained in both automated and manual form.

(C) Personnel records are maintained for the purpose of providing a history of payroll, promotion, discipline and related personnel information concerning Department employees.

(D) Personnel records are the responsibility of the Personnel Officer, whose business address is the Connecticut Department of Banking, 260 Constitution Plaza, Hartford, Connecticut. All requests for disclosure or amendment of these records should be made to the Personnel Officer.

(E) Routine sources for information maintained in personnel records are generally the employee, previous employers of the employee, references provided by applicants for employment, the employee's supervisor, the Comptroller's Office, the Department of Administrative Services, Division of Personnel and Labor Relations and State insurance carriers.

(F) Personal data in personnel records are collected, maintained and used under authority of the State Personnel Act, Chapter 67 of the General Statutes.

(2) Records maintained in connection with licensees, registrants and personnel of financial institutions.

(A) These records are maintained at the Connecticut Department of Banking, 260

Constitution Plaza, Hartford, Connecticut.

(B) These records are maintained in both automated and manual form.

(C) As authorized by the applicable state statutes, these records are maintained for the purpose of fulfilling the Department's licensing and other regulatory responsibilities.

(D) The Director of the Securities and Business Investments Division is responsible for the records pertaining to securities registration and licensing. The Director of the Bank Examination Division is responsible for the records relating to banking institutions. The Director of the Consumer Credit Division is responsible for the records regarding mortgage lenders, consumer collection agencies, small loan companies, sales finance companies and debt adjusters. Requests for disclosure or amendment of these records should be made to the appropriate director as mentioned above. The business address for each of these Directors is the Connecticut Department of Banking, 260 Constitution Plaza, Hartford, Connecticut.

(E) Routine sources for information maintained in these records are generally the licensee, the registrant, the applicant, State Police background checks, applicable licensing authorities in other states, the State Police Bureau of Identification and employers.

(F) Personal data in these records are collected, maintained and used under authority of the General Statutes: (i) Chapters 664 to 667, inclusive (Banking Institutions); (ii) Chapters 672 to 672c, inclusive (Securities); and (iii) Chapters 668 to 669, inclusive (Consumer Credit).

(d) **Categories of Personal Data**

(1) Personnel Records.

(A) The following categories of personal data are maintained in personnel records:

(i) Educational records.

(ii) Medical or emotional condition or history.

(iii) Employment records.

(iv) Marital status.

(B) The following categories of other data may be maintained in personnel records:

(i) Addresses.

(ii) Telephone numbers.

(C) Personnel records are maintained on employees of the Department of Banking.

(2) Records maintained in connection with licensees, registrants and personnel of financial institutions.

(A) The following categories of personal data are maintained in these records:

(i) Educational records.

(ii) Medical or emotional condition or history.

(iii) Employment records.

(iv) Marital status.

(v) Financial records.

(vi) Reputation or character.

(B) The following categories of other data may be maintained in these records:

(i) Addresses.

(ii) Telephone numbers.

(iii) Complaints and/or inquiries.

(C) These records are maintained on licensees, registrants and personnel of financial institutions.

(e) **Maintenance of Personal Data—General**

(1) The Department shall maintain only such personal data as is relevant and necessary to accomplish the lawful purposes of the Department. Where the Department finds irrelevant or unnecessary public records in its possession, the Department shall dispose of the records in accordance with its records retention schedule, and with the approval of the Public Records Administrator pursuant to Section 11-8a of the General Statutes, or, if the records are not disposable under the records retention schedule, request permission from the Public Records Administrator to dispose of the records under Section 11-8a of the General Statutes.

(2) The Department will collect and maintain all records with accurateness and completeness.

(3) Insofar as it is consistent with the needs and mission of the Department, the Department, wherever practical, shall collect personal data directly from the persons to whom a record pertains.

(4) All employees who function as custodians of the Department's personal data systems or who have access thereto are to be given a copy of the provisions of Chapter 55 of the General Statutes, Section 36a-21 of the General Statutes and these regulations, and a copy of the Freedom of Information Act, Chapter 3 of the General Statutes and any other state or federal statute or regulation concerning maintenance or disclosure of personal data kept by the agency,

(5) All such departmental employees are to take reasonable precautions to protect personal data under their supervision from the danger of fire, theft, flood, natural disaster and other physical threats.

(6) The Department shall incorporate by reference the provisions of the Personal Data Act and regulations promulgated thereunder in all contracts, agreements or licenses for the operation of a personal data system or for research, evaluation and reporting of personal data for the Department or on its behalf.

(7) The Department shall have an independent obligation to insure that personal data requested from any other state agency is properly maintained.

(8) Only employees of the Department who have a specific need to review personal data records for lawful purposes of the Department will be entitled to access to such records under the Personal Data Act.

(9) The Department will keep a written up-to-date list of individuals entitled to access to each of the Department's personal data systems.

(10) The Department will insure against unnecessary duplication of personal data records. In the event it is necessary to send personal data records through interdepartment mail, such records will be sent in envelopes or boxes sealed and marked "confidential."

(11) The Department will insure that all records in manual personal data systems are kept under lock and key and, to the greatest extent practical, are kept in controlled access areas.

(f) **Maintenance of Personal Data—Automated System**

(1) To the greatest extent practical, automated equipment and records shall be located in a limited access area.

(2) To the greatest extent practical, the Department shall require visitors to such limited access area to sign a visitor's log and permit access to said area on a bona fide need-to-enter basis only.

(3) To the greatest extent practical, the Department will insure that regular access to automated equipment is limited to operations personnel.

(4) The Department shall utilize appropriate access control mechanisms to prevent disclosure of personal data to unauthorized individuals.

(g) **Maintenance of Personal Data—Disclosure**

(1) Within four business days of receipt of a written request therefor, the Department shall mail or deliver to the requesting individual a written response in plain language, informing him/her as to whether or not the Department maintains personal data on that individual, the category and location of the personal data maintained on that individual and procedures available to review the records.

(2) Except where nondisclosure is required or specifically permitted by law, the Department shall disclose to any person upon written request all personal data concerning that individual which is maintained by the Department. The procedures for disclosure shall be in accordance with Sections 1-15 through 1-21k of the General Statutes. If the personal data is maintained in coded form, the Department shall transcribe the data into a commonly understandable form before disclosure.

(3) The Department is responsible for verifying the identity of any person requesting access to his/her own personal data.

(4) The Department is responsible for ensuring that disclosure made pursuant to the Personal Data Act is conducted so as not to disclose any personal data concerning persons other than the person requesting the information.

(5) The Department may refuse to disclose to a person medical, psychiatric or psychological data on that person if the Department determines that such disclosure would be detrimental to that person.

(6) In any case where the Department refuses disclosure, it shall advise that person of his/her right to seek judicial relief pursuant to the Personal Data Act.

(7) If the Department refuses to disclose medical, psychiatric or psychological data to a person based on its determination that disclosure would be detrimental to that person and nondisclosure is not mandated by law, the Department shall, at the written request of such person, permit a qualified medical doctor to review the personal data contained in the person's record to determine if the personal data should be disclosed. If disclosure is recommended by the person's medical doctor, the Department shall disclose the personal data to such person; if nondisclosure is recommended by such person's medical doctor, the Department shall not disclose the personal data and shall inform such person of the judicial relief provided under the Personal Data Act.

(8) The Department shall maintain a complete log of each person, individual, agency or organization who has obtained access to, or to whom disclosure has been made of, personal data under the Personal Data Act, together with the reason for each such disclosure or access. This log shall be maintained for not less than five years from the date of such disclosure or access or for the life of the personal data record, whichever is longer.

(h) **Contesting the Content of Personal Data Records**

(1) Any person who believes that the Department is maintaining inaccurate, incomplete or irrelevant personal data concerning him/her may file a written request with the Department for correction of said personal data.

(2) Within thirty days of receipt of such request, the Department shall give written notice to that person that it will make the requested correction, or if the correction is not to be made as submitted, the Department shall state the reason for its denial of such request and notify the person of his/her right to add his/her own statement to his/her personal data records.

(3) Following such denial by the Department, the person requesting such correction shall be permitted to add a statement to his or her personal data record setting forth what that person believes to be an accurate, complete and relevant version of the personal data in question. Such statements shall become a permanent part of the Department's personal data system and shall be disclosed to any individual, agency or organization to which the disputed personal data is disclosed.

(i) **Uses to be Made of the Personal Data**

(1) Employees of the Department who are assigned personnel and payroll responsibilities use the personal data contained in the Department's personnel records in processing promotions, reclassifications, transfers to another agency, retirement and other personnel actions. Supervisors use that personal data when promotion, career counseling or disciplinary action against such employee is contemplated, and for other employment related purposes.

(2) Authorized employees of the Department use records in connection with licensees, registrants and personnel of financial institutions in processing registration and license applications, processing financial institution applications, processing consumer complaints and as otherwise needed in enforcing regulations regarding those entities subject to the jurisdiction of the Department.

(3) The Department retains personnel records and records in connection with licensees, registrations and personnel of financial institutions according to schedules published by the Public Records Administrator, Connecticut State Library.

(4) When an individual is asked to supply personal data to the Department, the Department shall disclose to that individual, upon request, the name of the agency and the division within the agency which is requesting the data, the legal authority under which the agency is empowered to collect and maintain the personal data, the individual's rights pertaining to such records under the Personal Data Act and the Department's regulations, the known consequences arising from supplying or refusing to supply the requested personal data, and the proposed use to be made of the requested personal data.

(Effective May 20, 1987; Transferred April 24, 1995; Amended January 30, 1996)