Jurisdiction	Massachusetts
Date	4/20/22
Law Firm	Polsinelli (https://www.polsinelli.com/)
Title, Name	Elizabeth (Liz) Harding, Shareholder Allison Krause, Associate
Contact Information	eharding@polsinelli.com, akrause@polsinelli.com

Questionnaire

I. Law concerning protection of personal information

i. Does your state have a general law concerning the protection of personal information in the private sector at the present or in the near future? Yes.

ii. Does your state have a general law concerning protection of personal information in the public sector at the present or in the near future? Yes.

iii. Does your state have laws concerning protection of personal information which apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.) No.

*There is no comprehensive law regarding the protection of personal information in Massachusetts. However, there is one law and a corresponding regulation governing the protection of personal data of data subjects in Massachusetts: (A) Massachusetts's data breach notification law Mass. Gen. Laws 93H, as amended ("**MDBA**"); and (B) the corresponding regulation 201 C.M.R. 17.00, related to standards of protecting personal information ("**SPPI**"). The MDBA is similar to many other U.S. state laws regarding notification of data security breaches, but the SPPI is one of the only regulations in the United States requiring business to uphold certain standards related to the protection of personal data.*

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I(please add a reply column as necessary,):

The title of the law: *Mass. Gen. Laws 93H § 1, and the Standards for the Protection of Personal Information of Residents in the Commonwealth.*

URL:
https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section1
https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download

Enforcement status:
MDBA: Enacted on October 31, 2007, amended on April 11, 2019
SPPI: Enacted on November 13, 2009

① The definition of "Personal Information"	*Personal information ("**PI**") includes a resident's first name or first initial and last name in combination with any one or more of the following items:* *A. Social Security Number* *B. Driver license number or government-issued ID number; or* *C. Account number or credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.* *However, "Personal information" does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.*
② The scope in which the law applies	*The provisions of the MDBA are applicable to any public or private entity maintaining information on MA residents, whether or not organized or licensed under the laws of MA, while the SPPI applies only to private entities (and excludes any state agencies).*
③ The territorial scope	*The MDBA applies to data subjects located in Massachusetts; however, businesses operating outside of Massachusetts must also comply with the law.* *The SPPI applies to all businesses who maintain personal information of a resident of*

	Massachusetts, whether or not the business is organized or licensed under the laws of Massachusetts.

ii. If there are any special instructions about the laws, please describe them.

Notification Obligations. *In the event of a data breach of PI, businesses must notify affected individuals and the Attorney General.*

Protection of Personal Information*. All businesses that own or licenses PI about a resident of Massachusetts, shall maintain a comprehensive written information security program ("**WISP**"). Every WISP must:*

A. Designate one or more employees to maintain a comprehensive WISP;

B. Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing PI;

C. Evaluate and improve the effectiveness of the safeguards for limiting such risks, including, employee training, employee compliance with policies and procedures, and means for detecting and preventing security system failures;

D. Develop security policies for employees relating to the storage, access and transporting of records containing PI;

E. Prevent terminated employees from accessing records containing PI;

F. Impose disciplinary measures for violations of the WISP;

G. Oversee service providers by: (1) taking reasonable steps to retain third-party service providers that are capable of maintaining appropriate security measures; and (2) requiring such third-party provider by contract to implement and maintain such appropriate security measures.

H. Impose reasonable restriction upon physical access to records containing PI;

I. Include a process to regularly monitor the WISP to ensure that the WISP is operating in a manner to prevent unauthorized access to or use of PI;

J. Be reviewed at least annually; and

K. Include a process of documenting responsive actions taken in connection with any incident of a breach of security.

In addition, each business that electronically stores or transmits PI, must include in the WISP, the establishment and maintenance of a security system that at a minimum:

L. Secures user authentication protocols;

M. Secures access control measures;

N. Encrypts all transmitted records and files containing PI that will travel across public networks;

O. Monitors the system for unauthorized access to PI;

P. Encrypts all PI stored on laptops or other portable devices;

Q. Contains firewall protection and operating system security patches;

R. Contains up-to-date version of system security agent software, including malware and virus protection; and

S. Educates and trains employees on the importance of personal information security.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your state, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

The relevant provision is inapplicable.

(b) Data Quality Principle

While there is no provision specifying this principle, if an entity experiences an unauthorized acquisition of data that compromises the security, confidentiality or integrity of PI, such entity is required to notify the affected individuals, and if applicable the Attorney General inMassachusetts.

(c) Purpose Specification Principle

The relevant provision is inapplicable.

(d) Use Limitation Principle

The relevant provision is inapplicable.

(e) Security Safeguards Principle

The SPPI contains requirements for the WISP, including technical requirements for maintaining PI.

Also, if an entity experiences an unauthorized acquisition of data that compromises the security, confidentiality or integrity of PI, such entity is required to notify the affected individuals, and if applicable the Attorney General In Massachusetts.

(f) Openness Principle

The relevant provision is inapplicable.

(g) Individual Participation Principle

There is no private right of action under the MDBA, but a violation under the MDBA may also be a violation of Chapter 93A of MDBA, which could give rise to a private cause of action.

(h) Accountability Principle

Civil penalties may be brought by the Attorney General in Massachusetts for any violations. In addition, a business that experiences an incident requiring notice and involving social security numbers shall provide credit monitoring services at no cost to such affected residents for a period of not less than 18 months.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

None.

IV. Data Localization and Government Access

*While there is no rule regarding Data Localization and Government Access under the laws of Massachusetts, US companies may theoretically be subject to US government surveillance laws, such as Section 702 of the Foreign Intelligence Surveillance Act ("**FISA 702**"), and National Security Letter requests issued by the FBI under Executive Order 12333 ("**EO 12333**" and together with FISA 702, "**US Government Surveillance Laws**"). US government commitments and policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for other purposes, including commercial advantage.*

*If violations of FISA 702 have occurred, individuals, including Japanese citizens and residents, may seek redress for said violations under several US statutes. An individual who has been subject to unlawful surveillance under FISA may seek damages, punitive damages, and attorney's fees against the individual who committed the violation. In addition, there is a separate private right of action provision under the Electronic Communications Privacy Act ("**ECPA**") for compensatory damages and attorney's fees against the government for FISA Section 702 violations. Further, individuals may also challenge unlawful FISA surveillance through the Administrative Procedures Act, 5 U.S.C. § 702 (2018), which allows individuals "suffering legal wrong because of" certain government conduct to seek a court order enjoining that conduct. Thus, as described above, Japanese citizens or residents, may seek redress for violations of FISA Section 702.*

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

None.