地域	マサチューセッツ州
日付	2022 年 4 月 20 日
法律事務所	Polsinelli (https://www.polsinelli.com/)
役職名、氏名	Elizabeth (Liz) Harding, Shareholder Allison Krause, Associate
連絡先	eharding@polsinelli.com, akrause@polsinelli.com

質問事項

I. 個人情報保護に関する法律

i. あなたの国には、現在又は近い将来施行される予定の私的分野における個人情報保護に関する一般法はありますか。

ii. あなたの国には、現在又は近い将来施行される予定の公的分野における個人情報保護に関する一般法はありますか。

iii. あなたの国には、現在又は近い将来施行される予定の個別の分野に適用のある個人情報保護に関する法律はありますか。(ある場合は概要を教えてください。)

*マサチューセッツ州には、個人情報保護に関する包括的な法律はありません。しかし、マサチューセッツ州には、マサチューセッツ州内のデータ主体の個人データ保護を規定する 1 つの法律とそれに対応する規則があります。(A) マサチューセッツ州一般法 93H 節(Mass. Gen. Laws 93H)(以下、改正を含み、「**MDBA**」といいます。); 及び (B) これに対応する規則である、個人情報保護の基準に関する 201 C.M.R. 17.00 (以下「**SPPI**」といいます。) です。MDBA は、データセキュリティ侵害の通知に関する米国の他の多くの州法と類似していますが、SPPI は、個人情報保護に関する一定の基準を維持することを事業者に義務付けている、米国内でも限られた規制の一つです。*

I の(i)(ii)(iii)について全て「該当なし」の場合は IV に進みます。

II. 個人情報の保護に関する規程の基本情報

i. I で言及いただいた個人情報保護に関する法律について以下の空欄を埋めて下さい。

名称: *Mass. Gen. Laws 93H, 及び州の住民の個人情報の保護の基準*

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

施行状況:

MDBA: 2007 年 10 月 31 日制定、2019 年 4 月 11 日改正

SPPI:2009 年 11 月 13 日制定

① 「個人情報」の定義	*個人情報(以下、「PI」といいます。)には、個人のファーストネーム又はファーストネームのイニシャル及びラストネームの組合せに、以下の項目いずれか 1 つ以上を組み合わせたものが含まれます。* *A. 社会保障番号* *B. 運転免許証番号又は政府発行の ID 番号* *C. 口座番号、クレジットカード番号、デビットカード番号と、個人の金融口座へのアクセスを可能にするセキュリティコード、アクセスコード、パスワードとを組み合わせたもの* *なお、「個人情報」には、公開情報、すなわち、公に利用可能な情報から合法的に取得される情報、または、一般公衆が合法的に利用できるようにされている連邦、州又は地方政府の記録から合法的に取得される情報は含まれません。*
② 法律の適用範囲	*MDBA の規定は、マサチューセッツ州法の下で組織又は認可されているか否かにかかわらず、マサチューセッツ州の住民に関する情報を保有するあらゆる公的又は私的な団体に適用されますが、SPPI は民間団体のみに適用されます(あらゆる州機関には適用されません。)。*
③ 地理的範囲	*MDBA は、マサチューセッツ州に所在するデータ主体に適用されますが、マサチューセッツ州の外で事業を行っている企業もこの法律に従わなければなりません。* *SPPI は、マサチューセッツ州法の下で組織又は認可されているか否かにかかわらず、マサチューセッツ州の住民の個人情報を保有するあらゆる企業に適用されます。*

ii. 上記の法について特に言及すべき事項がございましたらその概要をご教示下さい。

通知義務 *PI の漏えいが発生した場合、事業者は、影響を受ける個人及び司法長官に通知しなくてはなりません。*

個人情報の保護 *マサチューセッツ州の居住者に関する PI を所有又は認可するすべての企業は、包括的な書面による情報セキュリティプログラム(以下「**WISP**」といいます。)を維持しなければなりません。すべての WISP は以下のとおりでなければなりません。*

A. 包括的な WISP を維持するために、1 人又は複数の従業員を指名すること。

B. PI を含む電子的、紙的又はその他の記録の安全性、機密性又は完全性に対する合理的に予見可能な内部及び外部のリスクを特定し、評価すること。

C. 従業員の研修、従業員の方針・手続の遵守、セキュリティ・システムの障害を検知・防止する手段など、かかるリスクを制限するための保護手段の有効性を評価し、改善すること。

D. PI を含む記録の保管、アクセス、及び輸送に関連する従業員向けのセキュリティ方針を策定すること。

E. 退職した従業員が、PI を含む記録にアクセスできないようにすること。

F. WISP の違反に対する懲戒措置を講じること。

G. 以下の方法により、サービスプロバイダーを監督すること。

(1) 適切なセキュリティ対策を維持することができる第三者サービス・プロバイダーを保持するための合理的な措置を講じること、及び (2) 契約により、当該第三者プロバイダーが適切なセキュリティ対策を実施し維持することを要求すること。

H. PI を含む記録への物理的なアクセスに合理的な制限を課すこと。

I. WISP が個人情報への不正なアクセスまたは使用を防止する方法で運用されていることを確認するために、WISP を定期的に監視するプロセスを含むこと。

J. 少なくとも年 1 回見直されること;及び

K. セキュリティ侵害の発生に関連して取られた対応措置を文書化するプロセスを含むこと。

さらに、PI を電子的に保管又は送信する各事業者は、少なくとも以下のようなセキュリティシステムの確立と維持を WISP に含めなければなりません。

L. ユーザー認証プロトコルを保護すること。

M. アクセス制御手段を確保すること 。

N. 公共ネットワークを介して送信される PI を含むすべての記録及びファイルを暗号化すること。

O. PI への不正なアクセスがないかシステムを監視すること。

P. ノートパソコン又はその他の携帯機器に保存されるすべての PI を暗号化すること。

Q. ファイアウォール保護及びオペレーティングシステムのセキュリティパッチを含んでいること。

R. マルウェア及びウイルス保護を含む、最新バージョンのシステムセキュリティエージェントソフトウェアが含まれていること。

S. 個人情報保護の重要性について、従業員を教育・訓練していること。

III. OECD プライバシーガイドライン

i. OECD プライバシーガイドラインの各原則を体現した法の規定があればその概要をご教示下さい。
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) 収集制限の原則

該当する規定はありません。

(b) データ内容の原則

この原則について明記した規定はありませんが、企業または 公共機関が PI の安全性、機密性、または完全性を損なうデータの不正取得を経験した場合、当該企業または公共機関は影響を受ける個人、およびマサチューセッツ州司法長官（該当する場合）に通知することが義務付けられています。

(c) 目的明確化の原則

該当する規定はありません。

(d) 利用制限の原則

該当する規定はありません。

(e) 安全保護の原則

SPPI には、PI を保有するための技術的要件を含む、WISP の要件が含まれています。

また、企業または 公共機関が PI の安全性、機密性、または完全性を損なうコンピュータ化されたデータの不正取得を経験した場合、当該企業または公共機関は影響を受ける個人、およびマサチューセッツ州司法長官（該当する場合）に通知することが義務付けられています。

(f) 公開の原則

該当する規定はありません。

(g) 個人参加の原則

MDBA に基づく私的請求権はありませんが、MDBA の下での違反行為は、MDBA の Chapter 93A の違反となる場合があり、私的請求権を生じさせる可能性があります。

(h) 責任の原則

違反があった場合、マサチューセッツ州司法長官により民事罰が科される可能性があります。さらに、通知を必要とし、社会保障番号に関わる事件が発生した事業者は、影響を受けた住民に対して、18 ヶ月以上の期間、無料で信用モニタリングサービスを提供しなければなりません。

ii. OECD プライバシーガイドラインの各原則が適用されない分野があればその概要を教えて下さい。

ありません。

Ⅳ. ガバメントアクセスとデータローカライゼーション

あなたの国において、包括的なガバメントアクセスやデータローカライゼーションのような、個人データの主体の権利に影響を及ぼすような仕組みはございますか。ある場合は、その内容をご教示下さい。

*マサチューセッツ州法にはデータローカライゼーションとガバメントアクセスに関する規定はありませんが、米国企業は理論上、外国情報監視法第 702 条(「**FISA 702**」)、及び行政命令第 12333 号(「**EO 12333**」。以下、FISA 702 と合わせて「**米国政府監視法**」といいます。)に基づいて FBI が発行する国家保障書簡の要請などの米国政府監視法の適用を受ける可能性があります。 米国政府の責任と政策により、情報収集は対外諜報目的に必要なものに限定されており、商業的利益を含むその他の目的で情報収集を行うことは明示的に禁止されています。*

*FISA702 違反が発生した場合、日本国民や日本の居住者を含む個人は、いくつかの米国法令に基づき、当該違反に対する救済を求めることができます。まず、FISA に基づく違法な監視の対象となった個人は、違反を犯した個人に対して損害賠償、懲罰的損害賠償、弁護士報酬を請求することができます。また、電子通信プライバシー法(「**ECPA**」)は、FISA702 違反に関して、政府に対して補償的損害賠償と弁護士報酬を求めることを可能とする別の私的権利規定を定めています。さらに、個人は、特定の政府行為のために「法的過誤を被る」個人がその行為を差し止める裁判所命令を求めることを可能とする行政手続法(5 U.S.C. § 702 (2018 年))に基づき、違法な FISA 監視に異議を唱えることもできます。したがって、上記のように、日本国民又は日本の居住者は、FISA702 違反に対する救済を求めることができます。*

V. データ保護機関

データ保護機関がある場合は、名称と住所をご教示下さい。

ありません。