In-Class Exercise 9

Kompliance Krew

Breakfast at Diffanies (Bad)" is a new chain of restaurants (circa 2022) offering the best coffee, breakfast and lunches in the MA area. They have 6 locations and have just launched an online app for online transactions and in person purchases, coupons and to track consumer purchases. They have hired your company to evaluate compliance with MA data protection Laws, including 201 CMR 17.00
They specifically need you to answer these questions for them:

1.Does BaD need to worry about consumer rights to access, modify or delete their information? Please explain.

As per MAlaws 201 CMR 17.00:
(2) Scope. 201 CMR 17.00 applies to all persons that own or license personal information about a resident of the Commonwealth.

17.03: Duty to Protect and Standards for Protecting Personal Information (1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

Possible answer: while Massachusetts law (201 CMR 17.00) does not specifically address consumer rights to access, modify, or delete their information, **BaD should take these rights seriously** to ensure compliance with broader privacy standards and to maintain consumer trust. If BaD ever operates outside of Massachusetts or handles customers from other jurisdictions, these rights will become essential for compliance.

2.As a small business, we heard we can be exempt from compliance with MA data protection regulations. Is that true? Please explain.

No, to answer this question, yeah certain limitations are different and flexible with small businesses for example as a small-scale business you will handle relatively less data involving the residents of Massachusetts so you can reduce the layer of access control but you can't exempt it at any level.
Therefore whatever scale you are in or the size of the customer it doesn't matter, you have to comply with MA data protection regulations fully.

3.If we comply with this regulation, do we need to comply with NYDFS Part 500 separately? Please explain

Under Section 500.19(a)(1), which is also referred to as the Small Business Exemption, smaller Covered Entities are exempted from certain enumerated requirements of Part 500 when a Covered Entity and all of its Affiliates ***combined*** have a total of **fewer than 20 employees** and independent contractors. When determining whether a Covered Entity and its Affiliates have fewer than 20 employees and independent contractors, all of the Covered Entity's employees and independent contractors and all of the Covered Entity's Affiliate's employees and independent contractors must be counted regardless of where any of the employees and independent contractors are located.

Note that Affiliate is defined very broadly in Section 500.1 as any individual or entity, including but not limited to any partnership, corporation, branch, agency or association, that controls, is controlled by, or is under common control with any other individual or entity, including but not limited to any partnership, corporation, branch, agency or association. For purposes of this definition, *control* means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

4.We had a minor issue a month ago with our employee file – it was sent via email to our former accounting firm. We ended the contract with them 3 months ago. The contract has strict clauses that mirror the MA regulation. We have not heard back from them, despite 3 emails and 2 calls made to them. What should we do?

In this situation it could be a potential breach and data leakage about the employees, even though they are former accounting firm, it could be potentially affect if the files goes into the wrong hands. We should do the following steps as follows.

- Prepare a document: The document should be created with a proper mentioning of the file names and other details about the contents of the file. Time of the email sent and exactly whent the contract ended with the accounting firm. Make sure this report is detailed and has the important information as it will be used for legal proceedings in the future if the actual breach happens.
- Assess the risk: What is the scope of the document and potential impact can be caused by the information leakage from the document, we need to aware of that for proper action. Make sure whether the document has confidential information like Social Security Number and Employee ID and possibly company's important credentials, if so make sure you are protecting those details in the database and ensure proper security actions in place.

Also check whether the file is encrypted while sending it to the firm or any type of encryption methods on place.

- Notify the company and employees: Create awareness to the employees who's information has been shared or possibly compromised, so that they can ensure and defend themselves if something goes wrong. For example they can change password and can be more alert.
- Seek Legal Advice: Make sure to consult with the legal department regarding the issue especially using Massachusetts regulations and how others can act regarding this for safeguarding both employees and company.
  Along with that Legal counsel can also provide guidance on any contractual obligations with the former accounting firm and how to proceed given their lack of response.
- Follow up with the firm: Draft the formal mail with the help of legal team and send a copy to the accounting firm to acknowledge about the file that has been shared, also emphasize that this is required under the terms of contract that we had previously and regulations as well.
- Reporting Obligations: Under Massachusetts law, if there is unauthorized access to personal information that poses a risk of identity theft or fraud, you may need to report the incident to the Massachusetts Attorney General's Office and the Office of Consumer Affairs and Business Regulation (OCABR)
  This step is necessary and should be taken if accounting firm didn't respond for 5 to 7 business days.