

June 25, 2025

Senator Michael Rodrigues, Chair  
Senate Committee on Ways and Means  
State House, Room 212  
Boston, MA 02133

Senator Cindy Friedman, Chair  
Senate Committee on Steering and Policy  
State House, Room 313  
Boston, MA 02133

Dear Senator Rodrigues and Senator Friedman,

On behalf of the Greater Boston Chamber of Commerce and our 1,200 members, I write to offer comments on S.2516, *An Act establishing the Massachusetts Data Privacy Act*. The Chamber and its members understand the importance of protecting consumers' personal data and privacy. The Chamber believes that easily understandable data protections, including protecting the data of minors, the ability of consumers to opt-out of certain data collection activities or correct data, and clear privacy notices for consumers, are common-sense policies for consideration.

However, to the extent the Legislature considers state-specific regulation, we urge consistency and requirements that closely mirror those adopted in the majority of other states. Because this legislation will create costs for businesses, and impact how they execute their services, data privacy is a complex, interconnected issue that impacts businesses, people, and our state's competitiveness. As a leader in innovation and technology development, the Commonwealth must avoid adopting unnecessary obligations that are incompatible with regulations in other states or federal, sector specific standards. Given these competitiveness concerns, we urge the committee to avoid profound negative consequences involving unnecessary litigation, unclear mandates and requirements, and costly implementation of measures that do not improve privacy protections.

We appreciate the opportunity to provide feedback to you both as you consider comprehensive data privacy legislation in the Commonwealth.

### **General Concerns**

As a threshold matter, the Chamber believes that data privacy regulation should be enacted at the federal level, providing a consistent, implementable set of rules and expectations across the nation. The use of data, commerce, and business transactions do not stop at state borders, and enacting state by state rules that dramatically differ create unnecessary costs and unpredictable, sometimes conflicting legal and regulatory standards for implementation. Recognizing a comprehensive federal approach may not be forthcoming, the Commonwealth should strive to embrace a statute that is interoperable among that vast majority of states that enacted legislation, providing a consistent standard of conduct for Massachusetts companies.

Unfortunately, S.2516 as drafted will make Massachusetts an extreme outlier for data privacy regulations, threatening key industries poised for growth and powered by our highly skilled workforce. We urge the Senate to make significant changes to S.2516 to create clear, understandable definitions, specific exemptions, and implementable legal standards. The goal of any data privacy bill should be to protect consumer data and the consumer experience – not provide the best legal foundation for plaintiffs in future litigation. This bill will not just impact technology companies, but every major industry in the Commonwealth as all industries embrace modern technology and develop the next generation of high-tech tools and should be approached with care.

We have serious concerns about the specific language in S.2516, which creates a confusing, conflicting, and sometimes indecipherable set of rules for data privacy regulation compared to every other state with privacy regulation. It will significantly hurt the Commonwealth's competitiveness, ability

to innovate in key industries supported by the Mass Leads Act and would particularly harm Massachusetts-based employers. The ambiguous approach in S.2516 will, by design, lead to costly litigation against many of our key industries beyond our technology companies – our retail, health care, life sciences, financial institutions, and even our higher education and nonprofit institutions will be likely targets. It represents the most cumbersome data privacy proposal in the country.

The Chamber believes there is a path to a comprehensive data privacy bill, and encourages the Senate to work with employers – those most impacted – in the drafting of a common sense, implementable bill that balances the protection of consumer data, a goal we share, with the recognition of how both consumers and businesses of all sizes utilize data in different ways, in different industries. Data privacy legislation will have a widespread impact and should be thoughtfully crafted with clear goals and outcomes. We welcome the opportunity to partner on the significant changes necessary to produce a workable statute.

### **Specific Concerns**

#### ***1) Private Right of Action***

The Chamber strongly opposes the inclusion of a private right of action in S.2516, which will be nothing short of a disaster for Massachusetts-based employers – particularly with the current drafting issues in the bill. A private right of action invites a maelstrom of litigation specifically targeting Massachusetts's businesses without improving the consumer protections proposed in the bill. Few jurisdictions across the nation have adopted a private right of action, meaning the Commonwealth would become a negative outlier for data regulation and nationwide target for lawsuits. Similar to other consumer protection issues, the Attorney General's office is the most appropriate office to regulate data privacy, with penalty thresholds consistent with such protections.

#### ***2) Clear definitions are necessary***

Several definitions, from the term "affirmative consent" to the definitions of "personal data" and "sensitive data" are unnecessarily broad, complex, or ambiguous as to provide little guidance on how the requirements of the bill will apply. Unnecessary language, from the word "affirmative" before the term consent (which is then subsequently defined), the inconsistent use of "data" throughout the bill creates ambiguity and confusion.

For example, the bill does not clearly exempt data from employees or independent contractors of a data broker, controller, processor, or third party. In lines 436-438, the bill attempts to do so, but qualifies the exemption "to the extent that the data is collected and used within the context of that role..." It is unclear what this means or who decides whether data is "within context." Is data related to an employee's benefits covered? This type of unnecessary qualification is one example of many throughout the bill that make the proposed statute make compliance difficult or impossible.

It is also unclear how data collected through business-to-business transactions, such as mergers or acquisitions, should be treated under S.2516. As you know, the merger of a business will involve an exchange of data related to employees, customers, products, and other critical elements of business functions. Clause (14) of subsection (a) of section 10 refers to transfer of assets in the context of a merger, acquisition, bankruptcy..." but is unclear in application. The Chamber recommends exempting all business-to-business transactions, including but not limited to mergers and acquisitions, from data privacy regulation as part of Section 3 of legislation, clearly indicating such transactions are out of the scope of the Act.

#### ***3) Lack of specific exemptions***

In many instances, consumer data is already regulated or protected by federal or state statute. Health care services must adhere to the Health Insurance Portability and Accountability Act (HIPAA). These institutions, such as hospitals, insurers, providers, research institutions and others navigating HIPAA

should be exempt from further regulation, particularly when there are conflicting standards (such as those included in S.2516).

Data level exemptions, or vague references to “limitations” are not effective or clear about how entities should comply with myriad privacy requirements. For example, data privacy protections for personal information collected by financial institutions are regulated by the federal government. It is therefore more appropriate to exempt all financial institutions subject to such regulation from state legislation. The Chamber supports the following exemption language:

A financial institution or an affiliate of a financial institution as defined by and that is subject to the federal “Gramm-Leach-Bliley Act”, 15 U.S.C. SEC.

The Senate should also consider a clear exemption for small businesses that will have difficulty complying with the robust requirements of S.2516, beyond gross revenue figures. For example, businesses with fewer than 500 employees in the Commonwealth should be exempt from the Act, and revenue thresholds should be increased to avoid unintended consequences on small employers.

In the above areas and in others, the Chamber urges the Senate to provide clear exemptions for entities that already comply with data privacy regulatory frameworks.

#### **4) *Unnecessary complexity***

Consistent with the above comments, S.2516 inserts unnecessary complexity and confusion into a data privacy framework. For example, the legislation creates 3 different paradigms for some type of exemption from state regulation: Subsection (a) of Section 3, beginning at line 393, exempting certain entities such as government; subsection (b) of Section 3, attempting to exempt 12 categories of data but not the specific institutions involved, and Section 10, specifying another long list of “limitations” on a variety of activities. While demonstrating the broad reach of S.2516 impacting almost every industry in the Commonwealth and the need to understand the nuances behind privacy regulation, this complex approach creates much confusion for compliance. Narrowing the scope of the bill and focusing strictly on consumer data protection can achieve data privacy goals in targeted approaches will lead to better and consistent outcomes.

The bill also regulates personal data, sensitive data, location data, and inferred data with different standards in different circumstances, with little consistency. While the Chamber is open to heightened protections for a concise, clear category of sensitive data beyond personal data, the combination of broad definitions and unclear standards in S.2516 again increases the costs and difficulty of compliance.

S.2516 requires controllers to “publicly commit to maintaining and using de-identified data...” creating some sort of required pledge to the goals of the legislation. A data privacy bill should create clear rules of conduct but should not (and arguably cannot) require statements of companies outside of required privacy notices, which would only be duplicative.

The Chamber urges the Senate to pursue a data privacy regulation approach that is clear, concise, and avoid duplication or unnecessary regulation that does not bolster consumer privacy.

#### **5) *Data minimization standard***

S.2516 creates a new legal standard, untested in the nation, for minimizing data collection. In lines 570-586, this standard will, as admitted by proponents, lead to expensive litigation against Massachusetts’ employers. The ambiguous language will require court interpretation – instead, we urge the Senate to adopt language consistent with peer states:

A controller shall limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as

disclosed to the consumer. Except as otherwise provided in this Act, a controller shall not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

#### **6) *Right to cure***

Given the widespread impacts and complex requirements of data privacy regulation such as S.2516, the Chamber urges the Senate to provide for a right to cure period for employers and businesses seeking to comply with the legislation. The Legislature, in partnership with the business community, regularly adopts such provisions when creating new areas of regulation, most recently as part of salary range transparency legislation last session. Other states such as Maryland have adopted a right to cure as they impose data privacy requirements and regulation. We urge the Senate to provide an opportunity to cure defects with the following language:

Notwithstanding any general or special law to the contrary, prior to January 1, 2030, before imposing any penalties or fines pursuant to this Act, the Attorney General shall provide a notice of violation to any person, controller, processor, or third-party alleging any violation of this Act. Such person, controller, processor, or third-party shall have at least 90 days to cure the violation after receipt of the notice, subject to the approval of the Attorney General. If the person, controller, processor, or third-party cures any violations within such 90 days, the Attorney General shall not impose any fines or penalties authorized by this Act.

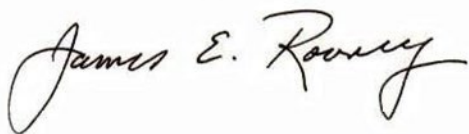
#### **7) *Privacy Notices***

While the Chamber supports disclosure of data collection and privacy policies and procedures by controllers, S.2516 creates overly complex and burdensome data privacy notice requirements. Subsection (c) of section 6 of proposed Chapter 93M outlines a dozen requirements for privacy notices instead of a straightforward disclosure of the personal data processed, the purpose for processing personal data, how to exercise consumer rights, and how to contact the controller regarding data use.

In sum, the Chamber believes that data privacy is important and recognizes a pathway to a commonsense bill that protects consumers' data without hurting the state's competitiveness. However, significant changes are needed to S.2516 to achieve that goal. The Chamber stands ready to partner with you to improve the legislation so it is workable and implementable while achieving important privacy goals for the Commonwealth.

Thank you for your attention and please reach out with any questions.

Sincerely,



James E. Rooney  
President & CEO