June 26, 2024

The Honorable Tracy Pennycuick
Chair, Senate Communications & Technology Committee
Senate Box 203024
Harrisburg, PA 17120-3024

Dear Chair Pennycuick:

BSA │ The Software Alliance[1] supports strong privacy protections for consumers and appreciates the Pennsylvania House of Representative's work to improve consumer privacy through House Bill 1201 (HB1201), the Pennsylvania Consumer Data Privacy Act. In our federal and state advocacy, BSA works to advance legislation that ensures consumers' rights — and the obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data. At the state level we have supported strong privacy laws in a range of states, including consumer privacy laws enacted in Colorado, Connecticut, and Virginia.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We appreciate the opportunity to share our feedback on HB1201. Our recommendations below focus on BSA's core priorities in privacy legislation: clearly distinguishing between controllers and processors, establishing practical obligations for processors, and ensuring HB 1201's interoperability with other state laws. We also urge you to revise the bill's short effective date, to provide companies with sufficient time to adopt compliance practices that comply with the bill's requirements.

---

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

I. Distinguishing Between Controllers and Processors Benefits Consumers.

We support HB1201's clear recognition of the unique role of data processors. Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction by assigning important — and distinct — obligations to both processors and controllers.[2] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.[3] This longstanding distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[4] BSA applauds the incorporation of this globally recognized distinction into HB1201.

Distinguishing between controllers and processors better protects consumer privacy because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data. Privacy laws should create important obligations for both controllers and processors to protect consumers' personal data — and we appreciate HB1201's recognition that those obligations must reflect these different roles. Distinguishing between these roles creates clarity for both consumers exercising their rights and for companies implementing their obligations.

II. The Bill's Provisions Giving Controllers an Opportunity to Object to Processors' Use of Subcontractors Should be Revised.

While HB1201 recognizes the important distinction between controllers and processors, we are concerned that some aspects of the bill could inadvertently limit processors' ability to provide consumers and businesses with the products and services they request, reduce their ability to safeguard those services, or even create privacy and security risks for consumers.

---

[2] *See, e.g.*, Colorado CPA Sec. 6-1-1303(7, 19); Connecticut DPA Sec. 1(8, 21); Delaware Personal Data Privacy Act, Sec. 12D-102(9, 24); Florida Digital Bill of Rights Sec. 501.702((9)(a)(4), (24)); Indiana Senate Enrolled Act No. 5 (Chapter 2, Sec. 9, 22); Iowa Senate File 262 (715D.1(8, 21)); Kentucky Consumer Data Protection Act Sec. 1(8, 22); Maryland Online Data Privacy Act Sec. 14–4601(K, Z); Minnesota Consumer Data Privacy Act Sec. 3(h, r); Montana Consumer Data Privacy Act Sec. 2(8,18); Nebraska Data Privacy Act Sec. 2(8, 24); New Hampshire Senate Bill 255 (507-H:1(IX, XXII); New Jersey Senate Bill 332/Assembly Bill 1971 (Section 1); Oregon CPA Sec. 1(8, 15); Tennessee Information Protection Act 47-18-3201(8, 20); Texas Data Privacy and Security Act Sec. 541.001(8, 23); Utah CPA Sec. 13-61- 101(12, 26); Virginia CDPA Sec. 59.1-575.

[3] *See, e.g.*, Cal. Civil Code 1798.140(d, ag).

[4] For additional information on the longstanding distinction between controllers and processors — sometimes called businesses and service providers — BSA has published a two-pager available here.

Specifically, Section 6(b)(4) creates significant concerns. It requires contracts between a controller and processor give the controller an "*opportunity to object*" to the processor's subcontractors.

We recognize the need for a consumer's data to be protected regardless of whether the data are held by a processor or by the processor's subcontractor. However, we strongly recommend a different approach: requiring processors to *notify* a controller about the use of a subcontractor and pass on the processor's obligations to that subcontractor — but not requiring controllers have the *opportunity to object* to subcontractors. This issue is particularly important, because of the frequency with which processors engage subcontractors to provide services requested by controllers. In many cases, processors will rely on dozens (or more) of subprocessors to provide a single service and may need to replace a subcontractor quickly if the subcontractor is not able to perform a service due to operational, security, or other issues. Requiring that controllers have an opportunity to object slows down the delivery of services and products to consumers, without clear benefits to privacy. Indeed, if a processor needs to switch subcontractors quickly because of a security issue, the delay involved in providing a controller the opportunity to object to a new subcontractor may expose consumers' data to security and privacy risks.

Instead of creating an opportunity for controllers to object to a processor's subcontractors, we recommend revising HB1201 to require a processor to notify a controller about subprocessors and pass on obligations to subcontractors via contract. This approach ensures consumers' personal data remain protected.

III.   Promote an Interoperable Approach to Privacy Legislation.

Finally, BSA appreciates efforts to align of many of HB 1201's provisions with the Connecticut Data Privacy Act (CTDPA). Privacy laws around the world need to be consistent enough that they are interoperable, so that consumers understand how their rights change across jurisdictions and businesses can readily map obligations imposed by a new law against their existing obligations under other laws. In particular, we support HB1201's exclusion of employment data from the bill's scope and in its definition of "consumer." We also support HB1201's approach to enforcement, which provides the Attorney General with exclusive authority to enforce the bill, which we believe will help promote a consistent and clear approach to enforcement.

At the same time, we are concerned that the bill provides an effective date of six months. We strongly encourage you to revise this provision of the bill, to ensure that businesses have at least a year to comply with the bill after enactment. All comprehensive consumer state privacy laws establish such effective dates,[5] which are important to drive businesses towards strong compliance practices that can better protect consumer privacy.

---

[5] BSA | The Software Alliance, Models of State Privacy Legislation, *available at* https://www.bsa.org /files/policy-filings/09192023stateprivlaw_0.pdf.

Thank you for the opportunity to provide our perspective in establishing strong consumer privacy protections. BSA would be happy to provide further perspective on this legislation as it progresses through the legislative process.

Sincerely,

Olga Medina,
Director, Policy