Business Software Alliance

The Honorable Kristen Gonzalez
Legislative Office Building, Room 817
198 State Street
Albany, New York 12247

June 2, 2025

Dear Chair Gonzalez and Members of the New York Legislature,

The Business Software Alliance[1] supports strong privacy protections for consumers. We appreciate your work to improve consumer privacy through Senate Bill 3044, the New York Privacy Act, but have significant concerns with how the legislation would work in practice.

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. In our advocacy, BSA works to advance legislation that ensures consumers' rights — and obligations imposed on businesses — function in a world where different types of companies play different roles in handling consumers' personal data.

We have significant concerns with S 3044, including its application to processors, which handle data on behalf of their business customers. Privacy laws worldwide, and all 20 comprehensive consumer state privacy laws, reflect the fundamental distinction between controllers, which decide how and why to collect consumers' personal data, and processors, which handle that data on behalf of other companies and pursuant to their instructions. Although S 3044 recognizes these different roles, it conflates their obligations — ultimately undermining privacy protections for consumers.

We strongly recommend revising S 3044 to:

- Reflect the role of processors, including their role in assisting controllers in responding to consumers' requests to access, correct, delete, and port their data.
- Not require processors to look at personal data they otherwise would not.
- Ensure the law's data minimization provisions do not freeze technology where it exists today.

[1] BSA's members include Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW Suite 310 Washington, DC 20001
202.872.5500 www.bsa.org

I. S 3044 Should Be Revised to Reflect the Role of Processors

Distinguishing between controllers and processors is a foundational aspect of privacy laws worldwide and in every state.[2] Controllers decide how and why to collect and use a consumer's personal information. Processors, in contrast, handle that personal data on behalf of a controller and pursuant to its instructions. Laws that recognize these different roles better protect consumer privacy by crafting different obligations for different types of businesses based on their different roles in handling consumers' personal data.

S 3044 appears to recognize the importance of this distinction by defining both controllers and processors. However, we are concerned that the bill imposes obligations that fail to reflect the role of processors — and may undermine the bill's goal to strengthen consumer privacy. We urge you to address at least five concerns:

- **The bill should be revised to reflect a processor's role in handling consumer rights requests**. As the bill recognizes, *controllers* must honor consumer rights requests, including requests to access, correct, and delete personal data. When that data is held by a processor, the processor's role is to assist the controller in responding to a request. The bill does not reflect that assisting role, creating significant concerns. Instead, it allows controllers to pass on consumer rights requests to processors, leaving too much room for consumer rights requests to fall through the cracks. For example, a processor won't know if data a consumer seeks to correct is inaccurate, or if a controller is legally required to retain data a consumer seeks to delete. We urge you to revise the bill to adopt the approach already in use under global and state privacy laws: require processors assist controllers by adopting technical and organizational measures to help a controller respond to consumer rights requests.[3]

    - <u>We strongly recommend</u>:
        - Removing references to processors in Sections 1202.6(c)(ii), 1202.7(a)(ii), and 1202.7(b), and instead
        - Revising Section 1203.1(f)(i)(E) to state that a processor must: Take appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to consumer rights requests.

- **Section 1203.2(c) should not require processors to review information on their services.** This provision imposes a "continuing obligation" for processors to review their ability to identify a specific natural person from the data they hold. Although it appears intended to protect data,

[2] Business Software Alliance, The Global Standard: Distinguishing Between Controllers and Processors in State Privacy Legislation, *available at* https://www.bsa.org/files/policyfilings/010622ctlrprostatepriv.pdf.

[3] For more information on a processor's role in handling consumer rights requests, *see* Business Software Alliance, Consumer Rights to Access, Correct, and Delete Data: A Processor's Role (Oct. 17, 2023), *available at* https://www.bsa.org/policy-filings/consumer-rights-to-access-correct-and-delete-data-a-processors-role.

it is likely to have the opposite effect. This would require processors to review data that belongs to their business customers — including large amounts of data they do not generally look at. That would upend privacy and security protections that processors routinely adopt, including contractual commitments not to review data on their services, except in specific circumstances. We encourage you not to adopt this requirement, which would have the counterproductive result of requiring processors to look at data they otherwise would not, undermining consumer privacy protections.

  - We strongly recommend striking Section 1203.2(c).

- **Section 1203.1(f)(i)(D) should not prohibit processors from combining personal data.** This requirement could prohibit companies from combining personal data in routine ways that benefit consumers. Indeed, controllers may ask processors to combine personal data to provide a product that a customer has requested, at the request of multiple businesses, or for a range of purposes that benefit consumers — without monetizing that data or using it for advertising. Combining data from multiple controllers is also essential to providing services at scale, including improving functionality of a product used by thousands of customers or offering cybersecurity protections based on data collected from a range of companies. It is important to ensure that controllers can direct a processor to combine personal data on their behalf and in line with their contract.

  - We recommend either deleting or revising Section 1203.1(f)(i)(D), to ensure processors may combine information received from one business customer to improve services offered to all business customers. This is a key part of offering services at scale.

- **Section 1203.1(f)(i)(I) should be removed, to ensure processors can protect consumers' personal data without unnecessary delays**. This provision requires processors to give controllers the opportunity to "approve or reject" subprocessors. While we agree that a consumer's data should be protected when it is handled by subprocessors, we strongly recommend a different approach: requiring processors notify a controller about the use of a subprocessor and pass on the processor's obligations to that subprocessor. This approach is already reflected in Section 1203.1(f)(i)(J). Requiring an opportunity to object is problematic, because a processor will often rely on dozens (or more) subprocessors to provide a single service. In some cases, a processor may need to quickly replace a subprocessor — like when a subprocessor has a security breach. In other cases, a processor may offer a service that depends on bringing together a specific group of subprocessors — so objecting to one subprocessor prevents use of the service altogether. We urge you to avoid these concerns by removing the opportunity to approve or reject subprocessors.

  - We strongly recommend deleting Section 1203.1(f)(i)(I).

- **Section 1203.1(f)(i)(B) should be revised to require processors to adopt reasonable security measures**. As written, this provision requires controllers to include a contractual requirement for processors to provide security measures "at least equal" to the controller's own measures. This assumes a processor will review a controller's publicly-available policies and then adopt cybersecurity measures aligned with each controller's separate policies. This does not reflect the fact that many processors offer services at scale to thousands of business customers. Rather than require a processor to adopt the same security controls as each of its business customers, we encourage you to require processors to adopt reasonable security measures.

    - We strongly recommend revising Section 1203.1(f)(i)(B) to state that a processor must "develop, implement, and maintain technical and physical safeguards reasonably designed to protect the security and confidentiality of personal data it processes on behalf of the controller in a manner consistent with the requirements of this article."

II. S 3044 Should Avoid Freezing Technology As It Exists Today.

We realize that S 3044 adopts a data minimization standard that is intended to limit the amount of personal data that companies use and retain. However, the bill does not clearly recognize that companies may need to process personal data to improve existing products they provide to consumers or to develop new ones that consumers are likely to want. As consumers, all of us want our technology to work better in 10 years than it does today — but the bill's language risks freezing technology in place, by failing to provide a clear path for product improvement and development.

- We recommend revising Section 1205.2 to add a new section stating that the obligations created by the bill do not restrict a controller's or processor's ability to: "conduct internal research to develop, improve, or repair products, services or technology."

* * *

Thank you for your continued leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you on these important issues.

Sincerely,

Kate Goodloe
Managing Director, Policy
Business Software Alliance