September 1, 2026

Business Software Alliance Recommendations on Bill C-36 (Privacy)

The Business Software Alliance (BSA)[1] welcomes the opportunity to provide feedback on the privacy protections created by Bill C-36 and the bill's implications for cross-border data transfers, which underpin the modern economy.

BSA is the leading advocate for the global software industry. Our members recognize the importance of privacy and security protections because our companies create the business-to-business products that help companies across the economy innovate and grow. BSA members provide tools including cloud storage services, human resource management software, identity management services, and cybersecurity products. As a result, privacy and security protections are a core part of BSA members' operations. Many BSA members have significant operations in both Canada and the US, with investments and employees in both countries.

We recommend revisions to eight aspects of Bill C-36:

- ***Role of service providers***. We strongly support the bill's recognition of the role of service providers — and recommend further improvements.
- ***Cross-border transfers.*** The bill creates new limits on cross-border data transfers, raising concerns for companies across industry sectors.
- ***Legitimate interests.*** The bill should encourage organizations to rely on legitimate interests, to promote responsible use of personal information without inundating consumers with consent requests.
- ***Automated decision systems.*** We appreciate new safeguards for automated decision systems but recommend defining them narrowly to avoid inadvertently sweeping in technologies like spreadsheets or routine security tools.
- ***Criminal penalties.*** We strongly recommend removing the bill's criminal penalties, which should have no role in enforcing privacy protections.
- ***Private right of action.*** We have significant concerns about the bill's duplicative enforcement regime, which allows individuals to bring private lawsuits after a regulatory investigation concludes.
- **Sharing threat information.** The bill should broaden its exception for sharing threat information about security incidents, to help organizations protect against bad actors.
- ***Children.*** The bill's definition of children as individuals under 18 is at odds with other global privacy laws and extends child-focused protections to teens.

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

We detail our concerns below as well as our recommendations. We would welcome an opportunity to further discuss these issues as you consider Bill C-36.

I. The Bill Recognizes the Important Role of Service Providers but Should Clarify Definitions.

Modern privacy laws worldwide distinguish between companies that decide how and why to collect or process a consumer's personal information (i.e., determine the means and purposes of processing) and companies that process information on behalf of a company that decides how and why the personal information is collected or processed. While many privacy laws refer to these roles as controllers and processors, Bill C-36 uses the terms organization and service provider. Recognizing these different roles is a core issue for BSA and we strongly recommend that any privacy law: (1) define these different roles, and (2) appropriately assign strong but different obligations to each type of entity, reflecting their different roles in handling consumers' personal information.

We welcome Bill C-36's express recognition of the role of service providers. Although the Personal Information Protection and Electronic Documents Act (PIPEDA) focuses on organizations, it also implicitly recognizes the role of service providers, including through guidance on how organizations should use contractual or other means to protect information when they engage service providers.[2] We appreciate that Bill C-36 expressly defines service providers, in addition to organizations. This clarity is critical because in the modern economy one organization may engage dozens of service providers to create the products its customers expect. Defining both organizations and service providers also ensures that a privacy law may assign different obligations to these different entities, based on their different roles in handling consumers' personal information. That improves protections for consumers, by ensuring all companies who handle their personal information protect it.

We recommend improving the definitions of both organizations and service providers. These definitions should more clearly distinguish between the two roles by recognizing that: (1) organizations decide how and why to collect consumers' personal information and, (2) service providers only process personal information on behalf of an organization and in accordance with the organization's instructions. These revisions would bring Bill C-36's definitions in line with the globally-recognized definitions of controllers and processors, which underpin modern privacy laws worldwide. These roles have been recognized for more than 40 years, including the OECD Privacy Guidelines, the APEC Privacy Framework, and ISO 27701.2.[3] We recommend the following changes:

- **Organizations** should be defined as entities that, alone or jointly with others, determine the purposes and means of processing personal information. This brings the bill's definition of organization in line with globally-recognized definitions of controller.

- **Service providers** should be defined as entities that handle personal information on behalf of an organization and pursuant to its instructions. This brings the bill's definition

[2] *See, e.g.*, Office of the Privacy Commissioner of Canada, Interpretation Bulletin: Accountability, *available at* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02_acc/.

[3] *See* BSA, Controllers and Processors: A Longstanding Distinction (last revised July 30, 2026), *available at* https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

of service provider in line with globally-recognized definitions of processor. *Importantly, service providers should not be defined as a subset of organizations, because doing so creates circular definitions that lead to circular requirements.*

These revisions support a globally-interoperable approach to key privacy terms, benefitting both Canadian companies operating globally and Canadian consumers using global services.

Recommendations:

- Revise the definition of organization to read:
  - *organization includes an association, a partnership, a person or a trade union that, alone or jointly with others, determines the purposes and means of processing personal information.*

- Revise the definition of service provider to read:
  - Service provider means an entity ~~organization, including a parent corporation, subsidiary, affiliate, contractor or subcontractor,~~ that provides services ~~for or~~ on behalf of an~~other~~ organization ~~to assist the organization in fulfilling its purposes~~.

II. Bill C-36 Should Not Create New Restrictions on International Data Transfers.

We support Bill C-36's objective of ensuring that personal information remains protected when transferred outside Canada. However, we strongly recommend that Bill C-36 be revised to preserve PIPEDA's current approach to supporting international data transfers through the accountability principle — without creating unnecessary barriers to responsible cross-border data flows.

Cross-border data transfers are an essential component of the modern digital economy. Organizations routinely rely on global cloud infrastructure, cybersecurity providers, fraud prevention services, customer support operations, and other specialized service providers located in multiple jurisdictions. Restrictions on cross-border transfers have a chilling effect on a country's economy because they impede domestic companies and other organizations from fully benefiting from these cutting-edge technologies. In many cases, global technologies also provide best-in-class security capabilities. Restricting the use of globally-based technology services can inadvertently undermine important privacy and security objectives.

BSA strongly supports PIPEDA's current approach to international data transfers, which relies on the accountability principle. For more than two decades, Canada's privacy framework has recognized that organizations may transfer personal information across international borders for processing, provided that the organization remains accountable for the information and implements appropriate contractual and organizational safeguards. This approach has allowed Canadian organizations to participate in the global economy while maintaining strong privacy protections.

We are concerned by Bill C-36's new limits on cross border data transfers — and its requirement for organizations to conduct an impact assessment before disclosing or transferring personal information outside of Canada. Although the bill does not identify the requirements for such assessments, companies can face significant burdens in conducting transfer impact assessments, including in the EU where such assessments are highly complex and fall disproportionately on individual businesses. We strongly recommend rejecting this approach.

Instead, we recommend retaining the approach in PIPEDA, which ensures an organization is responsible for personal information that it processes, regardless of where the information is located.

This approach would preserve strong protections for Canadians' personal information while ensuring that Canadian organizations can continue to leverage secure global infrastructure and participate effectively in the international digital economy.

If Bill C-36 nevertheless retains a requirement to conduct transfer assessments, it should be revised to adopt a risk-based and narrowly scoped obligation. For example, any requirement to conduct a transfer assessment should not apply to routine transfers of non-sensitive data or processing for low-risk activities. In addition, any transfer impact assessment should be clearly labeled as such. Currently, Section 57 refers to “privacy impact assessments” that are to be conducted before disclosing or transferring personal information outside of Canada. But the term “privacy impact assessment” is already used in Section 18(4) to refer to a different assessment for organizations that process personal information on the basis of legitimate interests. Using the same term for two distinct assessments creates confusion and should be avoided.

Most importantly, if these requirements are retained, Bill C-36 or future regulations interpreting its requirements should leverage the work companies have already done under other global data protection laws to ensure that personal information remains protected regardless of its location. Specifically, the use of leading international data transfer mechanisms, such as the EU Standard Contractual Clauses, the UK IDTA model, or the APEC Cross Border Privacy Rules, should be treated as satisfying any assessment obligation created by Bill C-36.

Recommendations:

- Retain PIPEDA’s existing approach to cross border data transfers, which rests on the accountability principle, to ensure that an organization is responsible for processing personal information regardless of where it is located.
- Remove Section 57’s requirement for organizations to carry out impact assessments before disclosing or transferring personal information outside of Canada.
- If the requirement for transfer impact assessments is retained, revise it to:
    - narrowly scope the obligation to specific activities and avoid applying this obligation to routine uses of non-sensitive personal information;
    - clearly label the required assessment as a transfer impact assessment, to avoid conflating it with the privacy impact assessment referred to in Section 18(4); and
    - treat compliance with leading global data transfer mechanisms such as the EU SCCs, UK IDTA, or APEC CBPRs as satisfying any requirement to conduct such an assessment under Bill C-36.

III. The Bill Should Promote Processing Based on Legitimate Interests.

BSA strongly supports recognizing the ability of organizations to process personal information on the basis of legitimate interests. Section 18(3) of the bill recognizes that organizations may collect, use, or disclose an individual’s personal information without their knowledge or consent if they do so for an activity in which the organization has a legitimate interest.

We are concerned, however, with several of the limits that Bill C-36 places on the ability to process data on the basis of legitimate interests, including the suggestion in 15(1) that consent remains the default legal basis and treats other bases as exceptions to a consent requirement. This implementation of legitimate interests is considerably more prescriptive than comparable international frameworks and would impose significant operational burdens without clear privacy benefits. We recommend revising Section 18(3) to encourage organizations to rely on legitimate interest as a lawful basis for processing, which can reduce the need for organizations to seek express consent from individuals and ensure that consent requests are reserved for situations where they are most meaningful.

We have three concerns:

First, the bill should revise its requirement to conduct a privacy impact assessment for any processing conducted on the basis of legitimate interests. While organizations should responsibly evaluate privacy risks, the decision to rely on a legitimate interest should not, by itself, trigger a mandatory privacy impact assessment (PIA). By contrast, the EU GDPR requires organizations relying on legitimate interests to conduct a balancing test between their interests and the rights of individuals, but it does not generally require a formal data protection impact assessment solely because the legal basis for processing is legitimate interests. Instead, under the GDPR data protection impact assessments are reserved for processing activities likely to result in a high risk to individuals. Bill C-36 should adopt a similar risk-based approach by requiring PIAs only when otherwise warranted based on the nature of the processing, rather than whenever an organization relies on legitimate interests.

Second, the bill should not require organizations to publicly identify the activities for which they rely on the legitimate interests exception in their privacy policies. While transparency is an important objective, this requirement would create substantial operational burdens by requiring organizations to continually update public-facing privacy notices as business operations evolve. Organizations frequently introduce, modify, or retire legitimate-interest processing activities as products and services develop. Requiring continuous public cataloguing of these activities would provide limited additional value to individuals while creating significant compliance costs and increasing the risk that privacy notices become lengthy, overly technical, and less useful. A more practical approach would require organizations to explain the categories of processing undertaken pursuant to legitimate interests, rather than maintaining an exhaustive and continuously updated list of individual activities.

Third, we are concerned that the limit in Section 18(3)(b) prohibiting reliance on legitimate interests where personal information is processed "for the purpose of influencing the individual's behaviour or decisions" may inadvertently limit important types of processing. As drafted, this language could be interpreted to encompass a wide range of commonplace software features and commercial practices, including product recommendations, personalization, fraud and security alerts, accessibility features, workflow prompts, search ranking, and AI-enabled assistance — all of which are intended, in some respect, to influence user decisions or behavior. For example, the current language could prevent a software company from providing a user with a personalized toolbar that prominently features the tools she uses most frequently. It also creates ambiguity around routine cybersecurity actions, like automatically blocking an unauthorized user’s access to a particular resource or isolating a suspected insider threat. If this language is interpreted broadly, it can prevent organizations from taking these actions, which are both common and automated.

We recommend either removing this provision or clarifying that it is intended to limit manipulative or deceptive practices, such as dark patterns — and does ***not*** limit ordinary product functionality, user-directed personalization, or automated security and fraud prevention activities. Narrowing this provision would provide greater legal certainty while preserving the bill's objective of protecting individuals from harmful or coercive uses of personal information.

Recommendations:

- Encourage organizations to process personal information on the basis of legitimate interests by:
    - not requiring a documented privacy impact assessment for each activity that relies on legitimate interests;
    - removing requirements to publish in the organization's privacy policy a specific list of activities that rely on legitimate interests; and
    - removing or significantly revising language limiting processing based on legitimate interests for activities that influence an individual's behavior or decisions. If this provision is retained, it should clearly not apply to ordinary product functionality, user-directed personalization, or automated security and fraud prevention practices.

IV. The Bill Should Narrowly Scope Obligations for Automated Decision Systems.

BSA appreciates the importance of ensuring that companies develop and use automated decision systems in responsible ways. However, it is important to ensure that obligations around automated decision systems are scoped appropriately, to avoid wrapping in an overly broad range of AI-related tools.

Bill C-36 defines automated decision systems broadly, to include any technology that "assists or replaces" the judgment of human decision-makers. We have significant concerns with using the term "assist" to define automated decision systems, because this definition is not tied to a subset of AI-related technologies but instead defined to include "technologies" that meet the definition. As a result, the number of software tools and services that could be encompassed by the proposed regulations is staggering.

By comparison, the EU's cautious regulatory approach to automated technologies is more pragmatic. For example:

- The GDPR's restrictions on profiling (in Article 22) only apply to automated decisions that produce a legal or similarly significant effect on individuals.

- Under the AI Act, even "high risk" obligations do not apply when AI technologies are used for narrow procedural tasks, to detect decision-making patterns and anomalies, or to perform preparatory steps for human evaluation.

We strongly recommend revising the proposed definition in Bill C-36 along similar lines, to focus on technologies that "replace or substantially replace" the judgment of human decision-makers. This will ensure the bill's obligations for automated decision-systems are appropriately focused on automated systems, rather than systems like spreadsheets that could assist a human in making decisions.

The bill should also expressly exempt automated tools that are primarily deployed for cybersecurity, system defense, and fraud prevention. To the extent that the bill treats automated security mechanisms, such as inline firewall blocking, sandboxing, and endpoint containment as automated decision systems it would handicap organizations in combatting cybersecurity attacks.

Recommendation:

- Revise the definition of automated decision systems to read:
    - Automated decision system means any technology that ~~assists or~~ replaces or substantially replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network, or a comparable ~~other~~ technique.
- Expressly exempt automated tools that are primarily deployed for cybersecurity, system defense, and fraud prevention from the definition of automated decision systems.

V. Criminal Penalties Should Be Removed.

Effective remedies are important to ensuring that individuals' privacy rights are sufficiently protected and organizations are deterred from violating their obligations. However, we have significant concerns with provisions in Bill C-36 that impose criminal penalties.

Simply put: criminal penalties do not have a useful role to play in data protection law. While they exist in some jurisdictions, criminal penalties for privacy violations are far outside of international best practices. Criminal punishment is disproportionate to the risks addressed by a privacy law. In BSA's view, the substantive requirements of a privacy law — combined with monetary relief and regulatory-led enforcement proceedings — are sufficient to protect individuals' privacy interests. In practice, when the processing of personal information results in harms that criminal laws are intended to prevent, existing criminal laws typically already provide sufficient penalties to prosecute and sanction them those activities — and no new penalty is needed under a privacy law.

We also have significant concerns with Section 145, which would impose criminal penalties for six types of violations, including recordkeeping, data retention, and limits on the use of de-identified data. By providing criminal sanctions for acts or omissions that lack criminal or malicious intent, these provisions go well beyond remedies that are necessary to compensate individuals for harm they suffer and to deter violations of the laws. We strongly recommend revising Bill C-36 to remove all criminal penalties.

Recommendation:

- All criminal penalties should be removed.
- Section 145 should be removed or revised to eliminate criminal liability.

VI. The Private Right of Action Should Be Removed.

Under Bill C-36, organizations will be subject to duplicative enforcement actions — first by the new Commission, then by private litigants. Section 132 allows individuals affected by a violation to sue the relevant organization after the Commission has investigated and either issued a final finding of contravention, entered into a compliance agreement, or secured a conviction.

This structure subjects organizations to several rounds of liability for the same offense. In addition, there is not a clear limit to the damages individuals can seek through the private right of action created by Section 132. We strongly recommend against this approach.

Recommendation:

- Remove the private right of action created by Section 132.

VII. The Bill Should Allow More Threat-Sharing About Security Incidents.

Section 40 permits organizations to disclose personal information without consent to reduce or mitigate harms from a breach. However, an organization is only allowed to make such a disclosure to organizations that have already been formally notified of a breach. This restriction does not reflect how real-time threat and vulnerability information should move between security providers, customers, and information sharing bodies. Restricting organizations from sharing threat information until a notification has been completed will ultimately undermine security — and conflicts with fast-moving incident response timelines and real-time operational defense standards supported by international bodies and the Canadian Centre for Cyber Security.

Although Section 40(b) also allows sharing "solely" for the purpose of reducing harm to "the individual" whose information is shared, this is also too narrow. In many cases, the goal of sharing is to prevent or reduce harm to other individuals and organizations, even if harm has already occurred to the individual whose information is shared. We strongly recommend revising Section 40 to allow such sharing, which benefits consumers and organizations.

Recommendation:

- Broaden Section 40's threat-sharing exception. This provision should permit organizations and recognized information-sharing bodies to share threat and vulnerability information, without first requiring a formal breach notification under subsection 59(1).

VIII. The Bill Should Focus Obligations for Children's Data on Children, Not Teens.

Bill C-36 creates additional protections for children, who are defined as individuals under 18 years of age. The upper age limit of 18 for "child" clashes with other data protection frameworks such as the EU's GDPR and the US Children's Online Privacy Protection Act. This could prevent some children — particularly teenagers — from accessing services, even when it is beneficial for them to do so.

***

Thank you again for the opportunity to provide our views on creating strong, uniform national privacy legislation. We welcome an opportunity to further discuss these issues.

Sincerely,

Kate Goodloe
Managing Director, Policy
Business Software Alliance