



August 5, 2019

Mr. Daniel Therrien
Privacy Commissioner of Canada
Office of the Privacy Commissioner
30 Rue Victoria
Gatineau, Québec, Canada
J8X 4H7

Via email to: OPC-CPVPconsult2@priv.gc.ca

Re.: Comments of BSA | The Software Alliance on OPC's consultation on consent requirement to transfer personal information for processing purposes

Dear Mr. Therrien,

BSA | The Software Alliance ("BSA") appreciates this opportunity to participate in the Office of the Privacy Commissioner's (OPC) consultation on consent requirement to transfer personal information for processing purposes.

Transfers for processing hold significant practical importance for BSA's members. Our members¹ are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing and artificial intelligence products and services. BSA members serve as data processors and controllers across the worldwide digital economy, and they have entered into contracts with business partners to address their compliance obligations and that reflect their relationships with individuals and other end users. Under these arrangements, companies have created globally scalable services that provide a high level of data protection.

The interpretation of transfers for processing in OPC's *2009 Processing Personal Data Across Borders Guidelines* ("2009 Transfer Guidelines" or "Guidelines") – in particular, the conclusion such transfers are not "disclosures" – are consistent with the text of Canada's Personal Protection and Electronic Documents Act (PIPEDA). Arrangements that ensure the organizations that collect data are responsible for its protection, regardless of where or by whom it is processed, appropriately protect users. The OPC's proposal to classify transfers for processing as disclosures would disrupt these arrangements and impose significant burdens on organizations and individuals without increasing privacy protections. BSA

¹ BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

therefore urges the OPC to maintain the interpretation set forth in the 2009 Transfer Guidelines.

I. The 2009 Transfer Guidelines Are Consistent with PIPEDA and Global Data Protection Practices

The OPC's position on consent for transfers for processing in the 2009 Transfer Guidelines is legally and practically sound. The Guidelines strictly and appropriately limit the circumstances that qualify as transfers for processing. Specifically, "[w]hen an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected."² Transfers that involve different purposes presumably are not "transfers for processing" and do not fall under the Guidelines' interpretation of "disclosure."

Support in the Text of PIPEDA

The text of PIPEDA supports viewing transfers for processing – as defined in the 2009 Transfer Guidelines – as part of the use of personal information, rather than as disclosures. Principle 4.1.3 introduces the term "transfer" to describe third-party processing situations, rather than using "disclosure," which appears throughout PIPEDA³. The use of "transfer" rather than "disclosure" in Principle 4.1.3 strongly suggests that these two terms are not synonymous.

In addition, Principle 4.1.3 explicitly provides that personal "information that has been transferred to a third party for processing" remains under the responsible organization's "possession or custody." This approach requires organizations transferring data for processing purposes to take appropriate steps to ensure that PIPEDA privacy requirements will be met even when data is transferred for processing. This provision makes it clear that all decisions about the use of personal information remain with the organization and further distinguishes a transfer for processing from a disclosure, in which the recipient of personal information acquires independent rights to determine the purposes and other conditions of processing.

Moreover, PIPEDA's consent requirements do not compel the conclusion that a transfer for processing is a disclosure. Consent for collection, use, or disclosure is valid under Section 6.1 if "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." The 2009 Transfer Guidelines provide helpful guidance toward this end by advising organizations to "be transparent about their personal information handling practices," including advising individuals that the organization may transfer personal information outside of Canada for processing.⁴ Organizations that follow this guidance will provide individuals with ample

² 2009 Transfer Guidelines at 5.

³ PIPEDA, Principle 4.1.3: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third-party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

⁴ See 2009 Transfer Guidelines at 8-9.

information about the roles of processors in uses of personal information for which they seek consent.

Finally, the 2009 Transfer Guidelines are consistent with the purposes of PIPDEA. Section 3 of PIPEDA recognizes that “technology increasingly facilitates the circulation and exchange of information” and declares that the obligations under Part I advance two goals: (1) protecting the privacy rights of individuals and (2) advancing “the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.”⁵ Third-party processing is widespread across many countries and economic sectors and, with appropriate transparency and safeguards, within the reasonable expectations of individuals.

Processing Safeguards in the 2009 Transfer Guidelines

The processing safeguards that the Guidelines recommend form a strong foundation for ensuring that the “comparable level of protection” for personal information transferred for third-party processing includes limiting uses to purposes for which the organization collected information. This comprehensive set of measures includes: (1) assessing a processor’s technical, administrative, and personnel-based data protection measures before making a transfer; (2) taking reasonable steps to prevent unauthorized uses or disclosures by the processor; (3) forming contracts with processors that include, among other things, the right to audit the processor’s handling of personal information; and (4) exercising such rights as appropriate.⁶

These safeguards are generally similar to practices that organizations follow in controller-processor relationships under the General Data Protection Regulation and similar frameworks. The overall effect of these safeguards in many instances is that third-party processors do not know what kinds of personal information they are processing on behalf of other organizations, or even whether they are processing personal information at all. For example, an organization might use a processor’s cloud service to store encrypted personal information that is never decrypted in the processor’s systems. Such arrangements do not fit under the notion of “making known” or “revealing” information to a third party, which forms part of the foundation for the OPC’s proposal to interpret transfers for processing as “disclosures.”⁷

Potential Trade Concerns Surrounding the OPC’s Proposed Interpretation

Finally, BSA urges the OPC to consider the implications of its proposed interpretation under Canada’s trade commitments. BSA strongly supports trade agreements that recognize the importance of data flows across national borders. Such agreements are critical to preventing data localization requirements and fostering the digital economy. Although trade agreements typically permit governments to enact exceptions in their domestic laws, such exceptions should not unnecessarily restrict data transfers and should be proportionate to the risks presented.

⁵ See OPC, Consultation on Transfers for Processing – Reframed Discussion Document (June 11, 2019), question 6 [“Reframed Discussion Document”].

⁶ See 2009 Transfer Guidelines at 5.

⁷ See Reframed Discussion Document (discussing “grammatical and ordinary sense of ‘disclosure’”).

II. Requiring Consent to Transfer Personal Information for Processing Would Impose Significant and Unnecessary Burdens on Companies and Individuals.

The OPC's proposed interpretation of transfers for processing would impose significant burdens on organization to meet new consent requirements, provide little benefit to individual privacy protections, and create uncertainty for many organizations.

Burdens on Organizations

Irrespective of the form of consent that would be necessary for transfers under the OPC's proposed interpretation, the burden on organizations would increase substantially. As discussed above, accountability is at the core of existing relationships between responsible organizations and the third-party processors that they use. In their roles as controllers, companies expend significant resources evaluating third-party processors before engaging them, as well as exercising oversight throughout the service lifecycle. Companies acting as processors have developed business, technical, and administrative processes that provide strong safeguards for personal information and support the data protection obligations of responsible organizations.

Requiring organizations to obtain consent to make transfers to processors would not add meaningfully to any of these protections, if at all, but it would require entities to develop new processes to obtain and record consent – potentially for each individual data transfer. In addition, organizations' operations and ability to serve individual and enterprise customers could be interrupted by individuals' refusal to provide consent.

Burdens on Individuals

BSA recognizes that consent is a central element of PIPEDA and commends the OPC's effort "to breathe life into the ways in which" consent is obtained.⁸ As the OPC has previously recognized, avoiding "information overload" at the individual level is a key element of achieving this goal.⁹

Requiring explicit or implicit consent for transfers for processing, however, is more likely to contribute to information overload than alleviate it. Asking individuals to provide explicit consent for third-party processing transfers could introduce an untold number of additional decisions for individuals to make, many of which would duplicate the processes that organizations use to maintain accountability for transfers. Alternatively, if consent to a transfer is implied, there would seem to be little difference between the 2009 Guidelines and the proposed interpretation in terms of facilitating the exercise of personal autonomy.¹⁰

The 2009 Transfer Guidelines' recommendations for transparency about transborder transfers are useful and potentially informative to individuals, but they do not mean that "elevating these elements to a legal requirement for meaningful transparency" would be a small matter for individuals or organizations.¹¹ There is a substantial difference between providing clear and understandable information about transfers as part of personal

⁸ OPC, Guidelines for Obtaining Meaningful Consent (May 2018).

⁹ See *id.*

¹⁰ See *id.* (criticizing practices that "make the control – and personal autonomy – that should be enabled by consent nothing more than illusory").

¹¹ See Reframed Discussion Document, question 7.

information use, as advised under the Guidelines, and ensuring that this information leads to meaningful consent for a given transfer. Moreover, PIPEDA ensures that mechanisms other than consent provide appropriate protections in the context of transfers for processing. In particular, the obligations of responsible organizations and processors under PIPEDA, including requirements for processing contracts and other accountability measures, provide strong protections for personal information that is transferred to third-party processors.

Uncertainty Arising from the OPC's Proposed Interpretation

As Question 6 in the Reframed Discussion Document makes clear, the OPC's proposed interpretation raises several challenging questions about what information organizations would need to provide to individuals and what kinds of consent organizations would need to transfer information for processing. If the OPC adopts its proposed interpretation, BSA recommends that it take steps to address the many questions that the interpretation would leave open. Particularly helpful clarifications would include (1) a statement by the OPC declaring that it is maintaining its existing guidance regarding transparency about transfers for processing¹² and (2) issue guidance that explains how PIPEDA's implicit consent provisions apply to transfers for processing.

* * *

In closing, BSA urges the OPC to maintain the 2009 Transfer Guidelines, which are consistent with PIPEDA as well as the practices that many organizations maintain to protect personal information that is transferred to third parties for processing. BSA would be pleased to provide further information or assistance as the OPC continues its consideration of these important issues.

Sincerely,



Leticia S. Lewis
Director, Policy
BSA|The Software Alliance

¹² See 2009 Transfer Guidelines at 8.