August 2, 2019

Privacy Commissioner of Canada
Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Sent by email: OPC-CPVPconsult2@priv.gc.ca

Dear Sir:

The Canadian Life and Health Insurance Association (CLHIA) appreciates this opportunity to provide feedback to the Office of the Privacy Commissioner of Canada (OPC) on its Reframed Consultation on Transfers for Processing as it revisits its interpretation on transfers of information under PIPEDA.

Overview

The CLHIA is a voluntary association with member companies which account for 99 per cent of Canada's life and health insurance business. Canada's life and health insurers are active in over 20 countries with 3 Canadian companies being among the 15 largest in the world. Our sector is a highly competitive and information-driven industry. Life and health insurers rely on the secure and uninterrupted flow of data across borders for a number of commercial and back-office functions, including client services, product development, and market research.

In order to remain competitive internationally, it is important that insurers have the ability to move data quickly and securely across markets. Consumer trust is paramount within the industry and insurers would suffer reputational risks if consumer data is not used properly or is not secure. The industry has been a leader when it comes to protecting the privacy of consumers.

That is why the life and health insurance industry in Canada supports free trade agreements as they extend our reach to new customers and markets and grow the Canadian economy at home. Canada is a mid-sized country that operates in a global trading economy. Free trade agreements provide sound, transparent frameworks under which companies can compete and grow internationally. Digital trade provisions, including cross-border data flow agreements, are key parts of these trade agreements. For example, the newly ratified Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) contains text that protects the digital economy by limiting restrictions on cross-border data transfers and prohibits data localization. Similar language has been included in the Canada-United States-Mexico Agreement (CUSMA). The new OPC expectations to obtain consent prior to transferring information for processing could be challenged under CPTPP and CUSMA.

Further, the life and health insurance industry engages in international forums such as the Organization for Economic Co-operation and Development, G7, and G20, among others, to develop high standards that strike the appropriate balance on data governance rules.

While it is important to update existing privacy rules and legislation in order to remain current and relevant in light of technological advances, we believe that fundamental changes should be left to elected members of Parliament. As you know, Innovation, Science and Economic Development Canada (ISED) recently published a position paper, entitled *Strengthening Privacy in the Digital Age*, which touches on the trust and privacy of data with new technologies. This current legislative review brings an extensive formal consultation process where any interested stakeholder can fully consider all potential consequences of any changes. We believe that this is the appropriate forum to address the concerns of the OPC on information transfers.

The following paragraphs provide technical considerations on the OPC's consultation for your consideration.

Reframed Consultation Paper on Transfers for Processing

Although the CLHIA is supportive when consideration is given to new ways to enhancing the privacy of consumers, we are concerned that the changes to the OPC's long established policy position pertaining to transfer for processing will have far reaching and unintended consequences. The OPC's new position that consent is required before the transfer of information for processing is such a significant shift from its current interpretation that, as stated above, it should be part of a broader discussion such as the one being undertaken by ISED. We therefore question this consultation's alignment with the federal government's work and underscore the risk to organizations of bearing the cost of amending practices when there exists a strong possibility that any amended guidelines may be short lived. Consequently, it may be beneficial for the OPC to focus its efforts towards providing ISED with solutions to the privacy challenges it currently faces rather than revisiting a past interpretation, which remains legally correct and provided the required consumer protection.

Notwithstanding, we wish to provide the OPC with industry comments and concerns. In short, we do not believe that the new OPC interpretation is correct nor will it produce the expected results of additional consumer protection.

Consultation process

Although we understand the OPC's interest in exploring its office's prior interpretation if it feels it is "likely not correct as a matter of law[1]"; we would caution against acting in haste. We submit that any intended changes, especially if they are as significant as requiring consent before transferring information for processing, should not be made before the completion of the federal government's PIPEDA review. There are no guarantees that when amended, the PIPEDA legal requirements will be in line with the OPC's new interpretation. Expecting organizations to follow an amended OPC guideline will penalize the most compliant organizations as they will invest significant resources (employee allotment, time, money etc.)

[1] As noted in your Reframed discussion document in the section entitled Transfers for processing under the current law

to change their current processes for what may only be a limited period of time without providing any additional consumer benefits.

As for the implication of the Equifax investigation, it is our understanding that the matter of consent for transfer of personal information was not at the heart of the issue. Rather, the organization ultimately failed to meet its obligations under PIPEDA's accountability principle to have in placed adequate data security safeguards and processes. We suggest that the OPC's new interpretation is not the most appropriate solution to resolve what was essentially an issue of accountability.

Consequently, to extend the conclusions drawn on the basis of the facts of the Equifax investigation beyond that investigation, would not do justice to the complexity of a matter that will have extensive ramifications for numerous Canadian businesses. The OPC's new interpretation would substantially affect not only the business of life and health insurers but also the Canadian business climate and global competitiveness generally.

Members of the CLHIA agree that PIPEDA needs to be updated to keep it current and relevant in light of technological advances. However, we do not believe that changes to the current rules applicable to the transfer of personal information to a third party for processing are necessary or would increase the protection of Canadians' privacy. Should such fundamental changes be required, they should be left to elected members of Parliament as the current legislative review brings an extensive formal consultation process where any interested stakeholders can fully consider all potential consequences of said changes.

The principle of consent in the context of transfers of information for processing

The OPC is now taking the position that a transfer of information should be considered a disclosure of information and consequently that consent is required prior to such transfer. Although we understand that, based on the Canadian Oxford English Dictionary definition (as reviewed by the OPC), the providing of information from one company to another may appear to be a disclosure. We believe this interpretation does not take into consideration the complexity of a transfer of information for processing in an actual business context. The information is not simply provided to a third party service provider for its own use, but rather transferred for a clear and predetermined purpose; a purpose for which the transferring entity has obtained consent from the individual whose personal information is being transferred and remains accountable for the information.

Therefore, although the transferring organization is not requiring a specific consent for the transfer of information, it remains entirely responsible for the treatment of the personal information in the hands of the service provider. If consent were to be required, there would be no obligation on the transferring organization to protect the information by "contractual or other means "to provide a comparable level of protection while the information is being processed by a third party."[2]". The information under the possession or custody of the service provider would be protected by that entity alone. Today, both entities bear responsibilities for the protection of that information. Therefore, the OPC's new interpretation would lessen the protection of individual's information when transferred to service providers.

[2] 2009 Guidelines p. 4 of the document under the Background section

Consequently, we maintain that the correct position is stated in OPC's 2009 Guidelines on Processing Personal Data Across Borders (2009 Guidelines) and the body of cases that support this position including those that predate[3] and follow the guidelines. The transfer of information for processing by a third party service provider is a "use" and not a "disclosure" and "*When an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected*"[4].

Therefore, it is the life and health insurance industry's position that the following statement in OPC's January 2009 Guidelines on cross-border data transfers of personal information is and continues to be correct: "assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required" (emphasis added).

Expecting another layer of consent is regressing

Although the principle of consent has a role to play in the transfer of information for processing, we do not believe, as stated above, that a specific express consent is required. In fact, requiring express consent would contradict the knowledge gained over the years as to what is an effective consent for consumers. Overburdening individuals with descriptions of all the organization's outsourcing practices does not enhance their understanding. Rather, it creates longer, complex consents and privacy policies that may not necessarily highlight the most important aspects to a consumer of the organization's processes. This approach may, in fact, reduce their understanding and increase the possibility that the individual is going to forego reading the descriptions altogether. We suggest that in keeping with the OPC's Guidelines for Obtaining Meaningful Consent, organizations should continue "to avoid information overload and facilitate understanding by the individuals…". We submit that consumers want their personal information to be appropriately safeguarded and used for purposes they know are related to acquiring the goods and services they choose. These needs are not better fulfilled by requiring an additional consent for the transfer of their information in the context of normal business processing.

Furthermore, this new position is especially problematic if it is to be applied to existing consumer relationships. If the OPC is expecting organizations to obtain an express consent to validate current business arrangements, this will, without a doubt, derail already established services provided to consumers when those services are outsourced. First, we expect the success rate of *retroactively* obtaining consent for a service that is already being provided to be extremely low. The consumer has no motivation to take a proactive action to confirm a service they are already receiving. It is to be expected that they would also be irate should an organization cease to provide services to request a retroactive consent. This approach would equate to limiting organizations' contractual freedom of their outsourcing arrangements and by the same token be detrimental to consumers who will no longer benefit from the economies of scale for operational activities and generally cause Canadian businesses to be less competitive internationally. For those reasons, any new interpretation cannot be expected to apply to existing relationship and services.

[3] PIPEDA Case Summary #313 and PIPEDA Case Summary #333

[4] 2009 Guidelines p. 5 of the document under section entitled What Do These Terms In Principle 1 Mean?

However, even if organizations are expected to obtain this new consent prospectively, the expectation will still be untenable. Different tracking and monitoring processes would be required to administer the received consent to take into account the different consent variations. This will be at the very least inefficient but most probably untenable to manage and certainly prohibitively expensive for most organizations.

This is especially true if organizations are expected to specifically identify all third party processors including sub processors to a consumer. Insurers may have relationships with hundreds of different services providers. Here are examples of service providers and outsourcing arrangements that may be used by an insurer over the course of a year:

- mailing houses
- cloud services (for uses such as storage of company and consumer data)
- medical underwriting services (such as MIB)
- risk assessment testing
- reinsurance
- specialized technology providers (ex. electronic claims submission services)
- pharmacy benefits provider
- investment managers
- doctor referral services
- paramedical services (ex. blood and others)
- employee assistance programs
- auditors
- market research organizations (ex. customer service satisfaction)
- internet content management services
- etc.

In some circumstances, insurers may have multiple relationships with service providers to provide the same type of service. In addition, if insurers are expected to obtain a new consent every time they change third party service providers and consumers are permitted to withdraw their consent each time they are asked to provide a new meaningful consent, it will be next to impossible for organizations to manage. This will create a nightmare of record keeping and transitional issues.

In addition, if each client must provide consent before any new outsourcing arrangements are contemplated, the negative answer of one client will make outsourcing impossible and will force organizations to keep the information internally resulting in giving individuals the power of imposing a disguised data residency obligation on the organization. Such a result would be cost prohibitive. The same logic would apply should any changes be made to any existing service provider arrangements.

These demands on consumers to provide consent (thereby requiring a positive action) will also come from several different businesses at various times. Constantly bombarding consumers with updated consent requests will create consent fatigue and render the consent meaningless by further disinteresting individuals from reading even the most relevant information thereby diluting the value of any consent process. We understand that this is the exact result the OPC wants organizations to avoid as expressed in your 2016 Consent and Privacy Consultation and in the more recent Guidelines for Obtaining Meaningful Consent.

The life and health insurance industry has worked very hard to find the right balance by providing sufficient and meaningful information to consumers to obtain consumers' valid consent to the organization's collection, use and disclosure of personal information while not overwhelming the consumer. After years of further reviewing and refining, our members believe they have reached this balance. The OPC's revised expectation will bring organizations of all sectors back to the first days of PIPEDA and of consent. This is not a desirable outcome and it must be avoided.

Type of Consent Required

We do not believe it is necessary to determine what level of consent (implicit or explicit) would be acceptable before a transfer of information can take place since the basis of our position is that additional consent is not required. We continue to support the expectations of the 2009 Guidelines that organizations should be transparent and "make it plain to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction.[5]"

Naming the exact location (e.g. naming the countries where the personal information is to be sent) was never an expectation in the 2009 Guidelines. It was specifically and rightfully noted that "The OPC recognizes the complexity of the electronic world and understands that it is often impossible for an organization to know precisely where information is flowing while in transit." Similarly, any expectation to include the names of the relevant service providers in the notice would create undue administrative burden without enhancing the value of the consent for consumers.

In addition, sharing names of service providers would expose business arrangements in ways that could be easily accessed by competitors. This could prove harmful to competition. Service providers may themselves object to being specifically named. Indeed they often purposefully keep a low profile to protect themselves against becoming prime targets for cyberattacks or security hacks. It will also be crucial not to add details to a notice to transform it indirectly into an implied consent as consent to use the individual's information has already been obtained and, again, we do not believe that a specific consent before processing is necessary but rather would be detrimental as explained above.

In addition, the use of such a precise notice would require amendments every time there is a change in the location or the name of the service provider. Regardless of the notice, it is important to remember that under PIPEDA Principle 4.1.3, the organization remains accountable for the information wherever or with whomever it may be and must have appropriate safeguards to protect the information.

Additional requirements

In the context of financial institutions (including CLHIA members), this requirement to protect the information is also enshrined in OSFI's Guideline B-10 (Outsourcing of Business Activities,

[5] 2009 Guidelines p. 8 of the document under section entitled What Should Individuals Expect?

Functions and Processes). Under said guideline, federally regulated entities are expected, amongst other things, to:

- *"Evaluate the risks associated with all existing and proposed outsourcing arrangements;*
- *Develop a process for determining the materiality of arrangements;*
- *Implement a program for managing and monitoring risks, commensurate with the materiality of the arrangements; …"*

To properly manage the risks associated with material outsourcing arrangements, federally regulated entities are specifically expected to address in their contract for services:

> *j) Confidentiality, Security and Separation of Property - At a minimum, the contract or outsourcing agreement is expected to set out the FRE's requirements for confidentiality and security. Ideally, the security and confidentiality policies adopted by the service provider would be commensurate with those of the FRE and should meet a reasonable standard in the circumstances. The contract or outsourcing agreement should address which party has responsibility for protection mechanisms, the scope of the information to be protected, the powers of each party to change security procedures and requirements, which party may be liable for any losses that might result from a security breach, and notification requirements if there is a breach of security.OSFI expects appropriate security and data confidentiality protections to be in place. The service provider is expected to be able to logically isolate the FRE's data, records, and items in process from those of other clients at all times, including under adverse conditions.*

Unfamiliar terminology in Canada

The CLHIA is also concerned about the introduction of expressions that are not part of the body of Canadian privacy legislation. Although we understand the concept of data controller/processor are inspired by the GDPR, we fear that not all Canadian organizations have the means to understand them and apply them appropriately. We are especially concerned for small and medium size enterprises (SMEs) that may not have the resources to monitor and understand foreign jurisdiction legislation and their terminology. However, since PIPEDA became applicable to organizations some 15 years ago, SMEs have learned to understand and how to comply with its requirements. In addition, there seems to be no need to borrow terms from foreign jurisdictions when, as stated, our legislation already addresses transfer of information across borders. If nothing else, this new terminology will conflict or appear to conflict with current concepts under PIPEDA and will lead to confusion.

Rationale for re-interpretation and corresponding benefits to individuals remain unclear

As stated above, we believe the OPC's long standing legal interpretation is correct. Therefore, we fail to understand the OPC's current interpretation. We do not believe consumer complaints have played a significant role in this new position and we have not found any such issues raised during the most recent PIPEDA review. Hence, it does not appear to be a matter of public policy. Should there be an emerging issue of broader public policy, it should be addressed by the Innovation, Science and Economic Development Minister.

The supplementary discussion document, suggests that this change of interpretation was prompted by OPC's recent Equifax investigation. However, we question whether having express consent to transfer personal information would have resolved or even avoided the problem. In fact, it is our understanding that the issue in this case was a lack of appropriate measures of safeguards. Therefore, we suggest that focus should be placed on the principle of accountability (e.g. 4.3.1) and for the OPC to continue its oversight efforts rather than modifying OPC's original interpretation with all the negative consequences that we have already stated.

In addition, we note that should this change be considered with the goal of resolving any possible adequacy issues with the GDPR, this solution may miss the mark as the approaches and concepts in both jurisdictions may not be interchangeable due to key differences that exist between the regimes. For example, mechanisms exist in the GDPR to support cross border dataflows without the need for consent. Once more, an in-depth review should be done through the legislative process to evaluate the need for any changes to meet GDPR adequacy requirements and to study the impact on all Canadian privacy legislation (provincial laws, public laws etc.).

Specific impact on the life and health industry

As already stated, this new OPC interpretation will have far-reaching implications on all Canadian organizations. However, particularly for our industry, the requirement to obtain specific consent for transborder of information will, amongst other things, create significant operational challenges, affect competitiveness and increase the costs of doing business. The following are examples of practices that will be greatly affected by the OPC's new interpretation.

a) Medical Expert Consultation

   Insurers will be precluded from sending a client's personal information to a third party medical expert for consultation even if the client has already consented to such services. This is an integral part of the administration of a complex or contested claim.

   The OPC, amongst other authorities, have supported insurers' ability to proceed accordingly in the past. If not given the appropriate tools to adjudicate the claim, an insurer cannot assess the validity of the claim and consequently, make a decision as to the validity of the claim and pay benefits expeditiously. An expectation to obtain additional consent hinders the insurer's normal business processes. This may lead to significant delays before a decision can be made as to the payment of benefits and consequently increase the amount of time that an insured has to wait for the insurer to assess the validity of a claim.

b) Locating Policy Owners to Obtain Consent

   Life insurance contracts are contracts of long duration. A contract dating back 80 years is not unheard of. Although there is a responsibility on the contract owner to advise the insurer of their location, there are circumstances where contract owners cannot be located. It would be a significant burden to obtain consent from these individuals as their whereabouts are often only provided by their beneficiary after their death.

A similar situation is possible for group insurance and retirement plans, where relevant communications are provided by the employer. Consequently, subject to receiving a communication from the retired employee, for example, insurers do not always have the contact information for those employees. It may prove impossible for both the employer and the insurer to obtain a consent when the employee is no longer working for the employer and has lost track of them.

c) Inability to leverage specific expertise

If organizations are forced to limit or entirely keep in-house processes that are now being outsourced, there will be important costs savings lost and unnecessary complexity added to any insurance business operations. Some of these arrangements allow insurers to leverage service providers' expertise thereby enhancing the client's experience. For example, travel insurers will often use out of country emergency assistance service providers. These specialists can receive claim notifications, collect the information necessary to submit a claim and notify the insurer to confirm eligibility for benefits of the traveller. This helps accelerate the process for the insurer to confirm eligibility on a case-by-case basis. Once the service provider receives confirmation of eligibility, the claim's management process can take place, e.g. obtain a claim form, authorize payments, provide alternatives to care, provide assistance for return home if required, etc.

d) Reinsurance

Reinsurance is a vital part of insurers' risk management. If it were impossible to obtain the consent of individuals to transfer their information to reinsure their contracts, insurers would be forced to shoulder the burden of all risks in their own portfolio. This would be detrimental to the industry as a whole since it is by spreading the risk that insurance companies can protect individuals whose coverage would be too great a financial burden for a single insurance company to carry. If restricted from reinsuring a significant amount of contract, a sole insurer may be unable to bare the liabilities of a significant claim.

Transfers of personal information to third party providers for processing have been part of everyday business for years in Canada. It is essential to understand that current processes would not meet the new OPC expectations. Insurers would need to overhaul their information practices including their privacy policies, notices and consent language because these processes were modeled according to the expectations set in the 2009 Guidelines. It would also include revisiting anew any changes made to policies and procedures in response to the new expectations set out in the January 2019 *Guidelines for Obtaining Meaningful Consent*. As for current contracts, they would need to be revisited and amended. This would create additional difficulties, as some third party contractors may not be willing to make the required changes or to altogether reopen their contracts possibly to avoid potential renegotiations of provisions they believed to be set. Such changes could take years to implement.

Misalignment with other privacy laws

No other jurisdiction in the world appears to require organizations to give individuals a choice as to whether their personal information can be processed by a third party service provider domestically or outside of the country of collection. Not even the GDPR.

To expect organizations to do so may put them in conflict with other applicable rules. For example, Ontario's PHIPA clearly establishes[6] that the sharing of information with an agent or service provider is considered a "use" of information and not a "disclosure". This also raises the question of the impact of the OPC's new interpretation on substantially similar provincial legislation and the potential for important inconsistencies across the country.

Longer term solutions for future law

As a general rule, CLHIA attempts to provide solutions along with any industry comments we provide when participating in consultations. However, in this case, we are hard pressed to propose solutions as we do not believe there is a need to change the longstanding OPC interpretation.

In addition, the tools necessary to address the concerns with the processing of personal information are already contained in PIPEDA under the accountability principle. We believe this approach is also more closely in line with other jurisdictions and consumer expectations. While consent continues to remain central in our legislation, we agree with the OPC's statement that "it needs to be supported by other mechanisms[7]".

Canadian consumers want user friendly processes. And while they are concerned with their personal information, when it comes to their information crossing borders, we believe their concerns are more about how that information is protected rather than the sole fact of its transfer. This is reflected in the 2018 Environics Research survey entitled *Attitudes Towards Data Privacy and Transparency* in which respondents have answered that[8]: "Canadians are most interested in knowing how companies keep their personal information secure, and how information is used. Of least concern is how companies work with third party providers". Digital processes are the future and organizations' ability to compete and provide the best service to their customers are closely linked to their ability to use all types of services including some that reside across our own borders. It is essential for Canada's financial health that it remains as such.

As we noted in our July 2016 submission to the OPC's Consultation Paper on Consent and Privacy, and in the comments we will soon present to ISED, there may be value in examining the concept of "legitimate business interest" and evaluating if its implementation has proven successful in the European Union. This approach could allow businesses to process personal information without additional consent if they can prove that the data processing is necessary for the purposes of the legitimate interests pursued by such organization. These interests would have to be balanced against other interests, which, in the PIPEDA context, could be tied back to what a reasonable person would consider appropriate in the circumstances.

---

[6] Section 6 (1) For the purposes of this Act, the providing of personal health information between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information or a collection by the person to whom the information is provided.

[7] OPC 2016-17 Annual Report to Parliament on PIPEDA and Privacy Act p. 17

[8] See p. 5 – 15% of the 2,000 individuals surveyed chose third parties as a topic of interest http://cjf-fjc.ca/sites/default/files/CMA%20-%20Attitudes%20towards%20Data%20Privacy%20and%20Transparency.pdf

As for the OPC's specific questions pertaining to the future of the law, we are in the process of carefully analysing ISED's in depth consultation paper. This review should be finished early in the fall. Consequently, it would be premature to attempt to provide you with responses before the close of your consultation. We would however be open to sharing the life and health industry comments made to ISED with the OPC when they are available.

Conclusion

We would like to once again thank you for providing us with the opportunity to participate in this consultation. We stand ready to provide further assistance on other OPC draft guidance affecting this industry.

Should you have any questions or require additional information, please contact me (416-359-2016 or aduval@clhia.ca).

Yours truly,

"Anny Duval"

Anny Duval
Senior Counsel, CLHIA