February 12, 2021

Comments by the Centre for Information Policy Leadership on the Government of Canada's Public Consultation on Modernizing the Privacy Act

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Government of Canada's public consultation on modernizing Canada's Privacy Act. In 2019, CIPL provided feedback to the Department of Justice in response to several discussion papers on the issue of modernizing the Privacy Act.[2] We also provided comments on the Innovation, Science and Economic Development Canada's (ISED) proposals to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA).[3]

CIPL's comments focus primarily on the issues covered in our previous responses, most notably on the following:

1. The Government of Canada should ensure that the requirements of the Privacy Act and PIPEDA (or its future proposed update under the Consumer Privacy Protection Act) are closely aligned to provide continuity between the public and private sector in the protection of personal information as well as accountability when data is shared between the public and private sectors;

2. As much as is sensible and possible, the Privacy Act should embrace and incorporate rights and principles from international privacy regimes such as the EU's General Data Protection Regulation (GDPR) to ensure global interoperability between privacy regimes;

3. The Privacy Act should provide federal public bodies with opportunities to use and disclose de-identified personal information;

4. The Privacy Act should adopt provisions rooted in organizational accountability, such as requiring federal public bodies to conduct privacy impact assessments and adopt privacy management programs;

5. The Privacy Act should contain enhanced transparency requirements; and

6. The Privacy Act should be amended to better facilitate regulators' ability to prioritize and meet their regulatory objectives and to effectively ensure compliance by government institutions.

---

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] See CIPL response to Justice Canada's Technical Engagement with Experts on the Modernization of Canada's Federal Privacy Act, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_justice_canadas_technical_engagement_with_experts_on_the_modernization_of_canadas_federal_privacy_act__21_augu.pdf.

[3] See CIPL Comments on Innovation, Science and Economic Development Canada's Proposals to Modernize the Personal Information Protection and Electronic Documents Act, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipls_comments_on_iseds_proposals_to_modernize_the_personal_information_protection_and_electronic_documents_act.pdf.

Comments

A. Comments on Proposal for Discussion No. 3: "Incorporating personal information protection principles from international models in the Privacy Act"

Aligning the privacy protections of the Privacy Act with both PIPEDA and other international models should be one of the key goals in modernizing the Privacy Act. Individuals should have actionable rights and their personal information should be given strong protections regardless of whether it is collected and processed by the public or private sector. As such, the Privacy Act should incorporate PIPEDA's principles-based approach to privacy protection, which will remain in place even if Canada chooses to adopt the recently-proposed Consumer Privacy Protection Act (CPPA). A principles-based approach allows for organizations to implement privacy protections in a flexible and context-appropriate manner, based on the actual risks associated with the information uses at hand.

In fact, context-appropriate and risk-based privacy protections are at the heart of organizational accountability, which, in turn, has been at the heart of Canada's approach to privacy protection under PIPEDA. The accountability-based model to privacy has served Canada well in regulating the private sector, and it should be applied to the public sector as well. It has cemented Canada's reputation as a pioneer and leader in promoting organizational accountability globally.

Additionally, amendments to the Privacy Act should consider the approaches taken by other countries, such as the GDPR, when regulating digital privacy to ensure global interoperability. The Privacy Act should harmonize as much as possible and sensible key concepts with other privacy laws to promote cross border global transfers. As we have seen recently with the EU Court of Justice's *Schrems II* decision that overturned the EU-U.S. Privacy Shield,[4] privacy laws governing the public sector, and individuals' rights with respect to the data in the hands of the public sector, can impact private sector cross-border data flows.

B. Comments on Proposal for Discussion No. 5: "Updating rights and obligations, and introducing new ones"

- **A right for the individual to be notified when his or her personal information is collected by a federal public body unless an exception applies**
- **A right to request that inaccurate personal information be corrected in a timely manner**
- **A specific principle to protect personal information with appropriate technical, administrative and physical security safeguards**

Many of the rights and obligations outlined in this section, such as the right to correction, the right for an individual to be notified when his or her data is collected, and an obligation to protect personal information with appropriate security safeguards, have become standard practice in global privacy laws and should all be incorporated into the Privacy Act. Including these rights and obligations would

[4] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems ("Schrems II"), July 16, 2020, available at http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=9710274.

further the goal of harmonizing the Privacy Act with both PIPEDA and other international privacy laws and frameworks.

- **Expanded access rights**

Expanding the right to access one's personal information to foreign nationals has become particularly relevant in the wake of the EU Court of Justice's *Schrems II* decision, which overturned the United States' adequacy decision in part because of its failure to provide adequate redress rights to EU citizens. Providing foreign nationals the right to access personal information alone might not satisfy the CJEU's redress standard, but it is likely a key component. Given the impact that the *Schrems II* decision has had on American companies' ability to transfer data across from the EU to the U.S., a failure to provide these access rights could impact Canada in the same way, damaging global data flows to Canada and Canadian businesses. This is particularly notable given that the EU Commission is likely to revisit Canada's adequacy decision for transfers to organizations governed by PIPEDA, and could rely upon the same logic used by the Court in *Schrems II* in its evaluation.

- **An obligation to contain personal information breaches and to subsequently notify the Privacy Commissioner and affected individuals in certain cases**

As we proposed in our 2019 comments, CIPL supports a data breach and notification requirement for government bodies. Such a requirement should mirror the private sector breach notification requirements in PIPEDA and employ the same harm threshold: federal public bodies that have experienced a data breach should be required to report to the Privacy Commissioner of Canada any breaches involving personal information if it is "reasonable in the circumstances to believe" that the breach creates "a real risk of significant harm to an individual."

PIPEDA defines "significant harm" to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." In addition, the relevant factors under PIPEDA to determine whether a breach creates a "real risk of significant harm" are (1) the sensitivity of the personal information; (2) the probability that the information will be misused; and (3) any other prescribed factor. CIPL believes that this standard is appropriate for both the private and public sector, however, we think it should be further clarified. Thus, we suggest that this standard should require consideration not only of the sensitivity and probability of misuse, but also its confidentiality and the volume of the data that has been breached to determine whether notice is required. As to confidentiality, for example, unauthorized access to information that is already publicly available, or was already known by the recipient, usually does not result in a level of risk requiring notification.[5] We also believe that any federal breach reporting standard for government bodies should follow as much as possible relevant guidance on data breaches from the OPC.[6]

Federal public bodies should also apply the same standard for notifying individuals of data breaches as the private sector. Under PIPEDA, private sector organizations must notify individuals about a

[5] See US Chamber of Commerce and Hunton Andrews Kurth, LLP, "Seeking Solutions: Aligning Data Breach Notification Rules Across Borders", available at https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html at page 22.

[6] "What you need to know about mandatory reporting breaches of security standards", Office of the Privacy Commissioner of Canada, available at https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

breach if it is "reasonable in the circumstances to believe" that the breach creates "a real risk of significant harm to the individual."

Under PIPEDA, a breach must be reported to the OPC "as soon as feasible after the organization determines that the breach has occurred." The same timing requirement applies to notification to individuals. Thus, PIPEDA does not impose a specific timing requirement (such as "immediately" or a specific number of days, as some jurisdictions do). Instead, it allows for flexibility in timing based on the "feasibility" of a report or notification, and an actual "determination" that a breach has occurred. CIPL agrees with that standard and recommends that the same flexible standard be applied to the public sector.

When it comes to the timing of notification of individuals, it is important to "balance the risk associated with inappropriate delays against rushed notifications."[7] Delayed notices may increase any risk of harm by not providing timely information for individuals to protect themselves. Premature and rushed notices may give organizations insufficient time to understand the nature and scope of the breach, may cause unnecessary alarm, result in consumers undertaking burdensome and unnecessary protective steps, and expose additional information to risk of compromise if the notice is made before data security is restored.[8] The standard set forth in PIPEDA gives organizations sufficient time to determine with reasonable or sufficient certainty that a breach has occurred. It also permits them to select the precise timing of the notification based on other relevant factors, such as whether notification would undermine a criminal investigation, pose a risk to national security or other issues, the presence of which would render the notification unfeasible.

As to the timing of reporting a breach to the OPC, it is important that the timing be no later than the notification to individuals because the regulator may be required to provide guidance and information to affected individuals and address relevant compliance issues by the reporting organization, whether it is public or private. By employing the same standard for notification of individuals and reporting to the OPC, PIPEDA ensures that both the OPC and individuals receive the required report or notifications at the same time. We would support employing that same approach for the public sector.

- **Certain rights relating to enhanced public awareness of interactions with automated decision-making systems (such as artificial intelligence tools)**

In the context of automated decision-making, the Privacy Act should ensure that the public is made aware of interactions with these systems, consistent with the Canada's Directive on Automated Decision-Making, particularly given that the CPPA is proposing similar requirements for the privacy sector. However, we do not recommend a different transparency standard than for other types of processing. Transparency standards in the law should be generally applicable to all data processing, focusing on the delivery of understandable, actionable and relevant information to individuals. These should apply to interactions with automated decision-making systems as they do to other types of data processing. CIPL agrees with the proposal that individuals should be made aware of what kind of data goes into AI and automated decision making models, how decisions generally are made, how to correct false information and how to remedy erroneous decisions. We also agree that exceptions to these transparency requirements should be made for certain uses of these technologies by law enforcement and national security if the disclosure could harm the public interest.

[7] *Supra* note 5 at page 24.
[8] *Id.*

C. Comments on "Proposal for Discussion No. 7: Allowing a greater role for "de-identified" personal information"

- **Allow federal public bodies to use and disclose de-identified personal information in a greater variety of circumstances**

As we noted in our response to ISED's white paper on amending PIPEDA, Canada should align its treatment of de-identified data with other privacy laws to protect privacy and enable innovation by both the private and public sectors. The proposed CPPA would provide clarity on the use of de-identified personal information, and the Privacy Act should follow suit. The Privacy Act should thus be amended to allow for the use of de-identified information without consent where the information is used or shared in the public interest. De-identification is an important measure for organizations to use personal information effectively while also protecting individual privacy. Accordingly, its use should be encouraged in the law.

Incentives for de-identification, in addition to exemption from consent, would be the ability to use the de-identified data for internal research or for AI development without having to set pre-defined retention periods, or to have the data subject to the exercise of individual rights such as access, correction and deletion.

The discussion paper rightfully points to the increasing ability to re-identify previously de-identified information through sophisticated techniques and asks whether re-identifying such data should be a specific offense. CIPL believes that in light of the fact that complete and permanent de-identification is increasingly difficult, technical de-identification techniques should be complemented by enforceable administrative, technical, physical and legal safeguards that prohibit attempted re-identification of personal information except for certain permissible purposes.

- **Define "de-identified" personal information**

CIPL supports a standard for de-identification plus safeguards that was articulated by the US Federal Trade Commission in 2012: Personal information should be subject to fewer privacy protections or legal requirements if (1) the data is not reasonably identifiable; (2) the company publicly commits not to re-identify it; and (3) the company requires downstream users of the data to keep it in de-identified form.[9] This standard could be translated to the Privacy Act to mean that anonymization or de-identification requires reasonable technical anonymization or de-identification in light of the purpose for which the information is being used, coupled with appropriate contractual and legal safeguards that ensure an enforceable obligation not to re-identify the information.

Finally, some re-identification is legitimate in a few specific circumstances and must be protected by appropriate exceptions. For example, in situations where genuine security research aims to test security measures and techniques, re-identification of data that has been de-identified should not be subject to penalties. Those carrying out such genuine testing could be obliged to inform the OPC first before going public with their findings. This would mitigate the risk of people making public disclosures that could negatively impact individuals and claiming a defense of security testing.

---

[9] U.S. Federal Trade Commission report, "Protecting Consumer Privacy in an Era of Rapid Change, Recommendation for Business and Policymakers," March, 2012 at 22, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

D. Comments on "Proposal for Discussion No. 8: Introducing stronger accountability mechanisms into the Act"

As we proposed in our 2019 comments on Privacy Act modernization, CIPL believes that the Privacy Act should formally adopt accountability measures such as obligations for federal public bodies to have a Privacy Management Program (PMP) and to undertake Privacy Impact Assessments (PIA). We welcome that the Government of Canada continues to consider implementing these measures into the Privacy Act in its current public consultation.

For many years, CIPL has promoted the concept of organization accountability as a key building block of effective privacy and data protection and has advocated for codifying many key components of organizational accountability such as PIAs and PMPs. We have discussed organizational accountability in detail in a number of white papers,[10] and have held several workshops and events with participants including global data protection authorities (DPAs) and policy makers.

- **An obligation to have a Privacy Management Program**

Comprehensive PMPs help to operationalize relevant privacy requirements, promote compliance and engender increased digital responsibility and trust among data subjects, and are equally relevant to both the public and private sectors. Effective privacy protections start with having the right processes and procedures in place to enable those protections. Privacy programs that encompass the core elements of accountability are necessary for delivering the appropriate compliance and trust outcomes in both the public and private sectors. Accordingly, the Privacy Act should include an obligation for all federal public bodies to have comprehensive PMPs.

One of the key features of an accountability-based approach to privacy protection is that it is scalable, flexible and adaptable to the data processing context at hand. Including an obligation for federal public bodies to undertake PIAs will allow them to base the features of their privacy programs on the specific privacy risks posed by their processing activities. Combined, the requirements for PIAs and PMPs will allow federal public bodies to deliver privacy that is tailored to their specific needs and the needs of those whose data they collect. These requirements would both enable the effective implementation of, and compliance with, applicable privacy protections, as well as enable monitoring of the effectiveness and improvement of these protections. They would also facilitate demonstrating the existence and effectiveness of these protections on request by relevant parties, such as the Privacy Commissioner, in an enforcement context.

---

[10] See CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", July 23, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", July 23, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; CIPL Accountability Q&A, July 3, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, June 3, 2020, available at https://www.informationpolicycentre.com/organizational-accountability.html.

A PMP should address all issues relevant to the proper governance of the entire data life cycle, from collection, use, storage, sharing and disposal. The core elements of an accountability-based privacy program are: leadership and oversight; risk assessment; policies and procedures; transparency, training and awareness; monitoring and verification; and response and enforcement. A PMP based on these core elements may be designed to implement the substantive requirements of a specific law, and may include additional measures that spell out general principles set forth in the law.

In the context of private sector compliance programs, we have elaborated on the specific tasks under each of the seven core elements of accountability. Each of these tasks is relevant and adaptable to the public sector, and a PMP of a federal public body should have policies and procedures in place that correspond to each of the following elements:

1. **Establishing leadership and oversight for data protection and the responsible use of data,** including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board.

2. **Assessing and mitigating the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk.

3. **Establishing internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals.

4. **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program.

5. **Providing training for employees** to ensure awareness of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

6. **Monitoring and verifying the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures and controls through regular internal or external audits and redress plans.

7. **Implementing response and enforcement procedures** to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

- **An obligation to undertake a Privacy Impact Assessment**

PIAs are a key component of a risk-based approach to data protection. As privacy risk is contextual, public sector organizations should understand and assess the risk that their data uses pose to individuals. As such, CIPL supports the inclusion of a requirement for federal public entities to conduct PIAs in the Privacy Act. However, the contours of this requirement should be carefully considered.

CIPL believes that public sector organizations should be required to conduct an initial high-level assessment of risk for any proposed data use to determine which uses should be subjected to or prioritized for a full-blown PIA. Such initial assessment could be aided by guidelines from the Treasury Board of Canada Secretariat and/or the OPC as to what might be high risk or low risk data uses, keeping in mind that such guidelines should be rebuttable by the results of the actual assessment. Adopting such an approach would ensure:

1. The requirement to conduct a PIA is built into the law in order to tackle the currently uneven approach of conducting PIAs across federal public entities;
2. A timely process for conducting and prioritizing the most important government PIAs by ensuring that more focus is placed on assessing and mitigating high risk processing activities; and
3. The OPC spends time and resources reviewing only pertinent and truly risky processing activities.

CIPL believes that the test to determine when a PIA is required should be sufficiently broad and focus on the likelihood and size of the risk proportionate to the benefits of the processing. Additionally, the 2019 Directive on Automated Decision-Making already requires an "Algorithmic Impact Assessment," so a PIA requirement would help to harmonize privacy protections.

E. Comments on "Proposal for Discussion No. 9: Modernizing transparency practices"

- **New proactive publication requirements**

CIPL believes that user-centric transparency is foundational to effective privacy protections and fostering trust. As stated earlier, transparency is a crucial component of any privacy management program, and the Privacy Act should include provisions that require federal public entities to publish information about their PMP, PIAs, and information sharing agreements.

- **Enhancing transparency around indirect collections and secondary uses.**

It is essential that all organizations, whether in the public or private sector, be required to disclose their collection and processing practices, including indirect collections and secondary uses of data not known at the time of collection. Transparency surrounding indirect collections and secondary uses is particularly important because such data uses illustrate key examples of situations where a user would likely be completely unaware of the collection or processing, save for a transparency requirement. Transparency for these sorts of practices is essential to developing public trust.

F. Comments on "Proposal for Discussion No. 11: Creating an enhanced compliance framework to address unresolved issues"

CIPL supports the premise that for privacy rights to be effective, they must be supported by strong legal recourse and remedies. As we noted in our white paper "Regulating for Results: Strategies and Priorities for Leadership and Engagement" (Regulating for Results),[11] we believe that a results-based approach to data protection provides the foundations for effective regulation. Providing the Privacy Commissioner with additional powers to more effectively address complaints and pursue

[11] See CIPL White Paper on "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

investigations while also promoting constructive engagement outside of the enforcement context between the Privacy Commissioner and industry would be consistent with this results-based approach.

- **Giving the Privacy Commissioner the discretion to decline to investigate a complaint or to discontinue an active complaint investigation**

The Privacy Commissioner should be given discretion to decline to investigate a complaint or to discontinue an active complaint investigation. The complaint-handing role of a Data Protection Authority (DPA) provides recourse for individuals and valuable insights for DPAs on data usage and data protection practices, but it should not be given excessive priority over other duties of the Privacy Commissioner. Cases must be chosen carefully to prevent overwhelming the OPC with individual complaints that will drain its limited resources. As explained in our Regulating for Results white paper, regulators should be able to concentrate on and prioritize significant violations for enforcement, those whose resolutions will have the greatest impact on individuals, organizations engaging in potentially similar practices, and society.

In revising the Privacy Act, the Department of Justice Canada should consider the experience of European DPAs that have been inundated with complaints since the GDPR went into force. According to the EDPB, over 144,000 queries and complaints were made to European DPAs during the first year of the GDPR.[12] Moreover, during 2019-2020, the UK Information Commissioner's Office resolved 39,860 data protection complaints.[13] While there may be fewer complaints made to the OPC concerning government institutions versus private sector organizations, the OPC will need to consider the complaints it receives in the aggregate and as a result, the combined number of complaints may lead to swamping of the Privacy Commissioner if it does not have the discretion to decline to investigate complaints, particularly those that are frivolous or vexatious.

It should be for the OPC to decide which complaints merit a thorough investigation by analyzing the complaints it receives, allocating its limited resources appropriately and prioritizing its regulatory objectives.

The Privacy Commissioner should have the discretion to discontinue an investigation for the following reasons:

1. The government institution in question may have remediated the issue and resolved the complaint that led to the investigation rendering the ongoing investigation moot;

2. The OPC may have discovered that a complaint which looked meritorious on its face turned out to be frivolous or vexatious and no longer wishes to spend its limited resources investigating the complaint; and

3. The government institution may have made public statements outlining the reasons it was investigated by the OPC and the corrective actions it is now taking, rendering the continued investigation unnecessary.

[12] See 1 Year GDPR – Taking Stock, European Data Protection Board, May 22, 2019, available at, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.
[13] UK Information Commissioner's Annual Report and Financial Statements 2019-20, July 2020, available at https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

- **A public education mandate for the Privacy Commissioner (Annex 4.2)**

CIPL supports the inclusion of a mandate for the Privacy Commissioner to engage in public education activities aimed at the general public, akin to the Commissioner's powers under PIPEDA. Education and outreach efforts form a key component of the leadership function of DPAs and such functions should be given top strategic priority in the modern digital economy and regulatory landscape. As CIPL has previously noted in its paper on Regulating for Results, it is fundamental that DPAs engage directly in dialogue and take the lead in providing the information, advice and support which will make a practical reality of data protection.[14]

The Privacy Commissioner already engages in similar activities under the current mandate under PIPEDA. Such education and outreach efforts are equally as important for the public sector and CIPL supports aligning the mandate of the revised Privacy Act with respect to research and education with the Privacy Commissioner's authority under PIPEDA to engage in such activities.

DPAs in Europe already engage in such education and outreach efforts at the public sector level. The GDPR applies to public and private sector organizations with negligible distinction and much of the guidance produced by European DPAs is equally relevant for public authorities and government institutions as it is for the private sector. Moreover, the European Data Protection Supervisor (EDPS), an independent supervisory authority is specifically tasked with ensuring that EU institutions and bodies respect data protection rules when processing personal information and developing new policies.

- **Permitting federal public bodies to seek the Privacy Commissioner's views outside an investigation context (Annex 4.2)**

CIPL also believes that federal public bodies should be permitted to seek the Privacy Commissioner's views outside of an investigation context. Tools such as advance rulings and advisory opinions can help government institutions ensure compliance with the Privacy Act. They also can assist the OPC in ensuring proactive privacy protections for individuals while advancing constructive engagement with the bodies it regulates.

The leadership function of DPAs places emphasis on ensuring as much constructive engagement as possible between DPAs and those they regulate. In practice, constructive engagement involves many different activities, including maximum consultation to foster a "no surprises" approach to oversight. By permitting the OPC to engage in advance rulings, federal public bodies will be able to engage in beneficial dialogue with the Privacy Commissioner to understand what the right thing to do is in any novel processing context. Advance rulings also facilitate proactive data protection compliance rather than after the fact corrective action.

Additionally, other federal public bodies in Canada already have the ability to issue advisory opinions. Given the ever-increasing use of personal information by government institutions, CIPL strongly recommends providing the OPC with similar authority. Granting such authority is further supported by the fact that advance rulings are already possible at the provincial level.

[14] *Supra* Note 11 at page 30.

- **Introducing a "regulatory sandbox" environment (Annex 4.2)**

Constructive engagement can also function in a regulatory sandbox environment by creating a space for responsible innovation. CIPL has discussed the benefits of regulatory sandboxes in our white paper "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice."[15] Internationally, several DPAs, such ask the UK's Information Commissioner's Office, are using regulatory sandboxes to provide advisory opinions to organizations on specific projects that involve the processing of personal information and particularly complex data protection issues.[16] Regulatory sandboxes could thus provide an avenue for issuing advanced rulings.

Conclusion

Thank you for the opportunity to submit these comments and for considering them. If you would like to discuss any of our comments or require additional information, please contact Markus Heyder, mheyder@hunton.com; Matthew Starr, mstarr@hunton.com; or Sam Grogan, sgrogan@hunton.com.

[15] CIPL white paper on "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice, March 8, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

[16] See the UK Information Commissioner's Office regulatory sandbox beta phase initiative, available at https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/.