BLG

Submission on Guidelines for **Valid Consent**

Privacy and Data Protection Group | Montréal

Eloïse Gratton, Elisa Henry, François Joli-Cœur, Simon Du Perron, Julie M. Gauthier, Andy Nagy, Daniel-Nicolas El Khoury, Candice Hévin et Catherine Labasi-Sammartino

Authors' presentation

Eloïse Gratton

Partner and National Co-Leader,
Privacy and Data Protection
egratton@blg.com

Elisa Henry

Partner and National Co-Leader,
Privacy and Data Protection
ehenry@blg.com

François Joli-Cœur

Partner
fjolicoeur@blg.com

Simon Du Perron

Associate
sduperron@blg.com

Julie M. Gauthier

Counsel
jugauthier@blg.com

Andy Nagy

Associate
anagy@blg.com

Daniel-Nicolas El Khoury

Senior Associate
delkhoury@blg.com

Candice Hévin

Associate
chevin@blg.com

Catherine Labasi-Sammartino

Associate
clabasisammartino@blg.com

* Unless otherwise noted, the sections cited in this submission correspond to the sections of ARPPIPS and the Access Act as amended by the Act to modernize legislative provisions as regards the protection of personal information ("**Law 25**").

Q.1 What is your overall assessment of the draft Guidelines?

We welcome the Commission d'accès à l'information's ("CAI") efforts to facilitate the application of the Access Act[1] and the ARPPIPS[2] through these Guidelines on the criteria for valid consent. However, we are concerned that certain interpretations and examples found within the Guidelines may lead to confusion rather than clarity for organizations, potentially exacerbating the issue of consent fatigue[3] rightly decried by the CAI[4]. Therefore, our suggestions aim to ensure that the Guidelines provide clear and pragmatic guidance that is consistent with the applicable legal framework.

In the context of the ARPPIPS, where consent is the sole legal basis for processing personal information, it is important that the notion of consent not be interpreted in a way that is unduly rigid or unnecessarily burdensome for organizations, namely by requiring express consent more often than is necessary. This overemphasis on express consent can disrupt the user experience and lead to "consent fatigue." The CAI's interpretation, particularly with respect to profiling and other technological functions, at times appears to go beyond the intent of the ARPPIPS and may impose unfounded obligations. This could lead to an increase in consent requests in various industries that rely on cookies and similar technologies, mirroring the challenges faced under the EU's strict cookie laws. Given the ongoing debate within the EU about the practicality and effectiveness of such an approach[5], it is imperative that the CAI revise its interpretation to more closely align with the spirit and letter of the ARPPIPS. Doing so would strike a better balance between respecting the privacy rights of individuals and recognizing the operational realities of organizations, thereby allowing for a more meaningful and practical application of consent requirements.

The current Guidelines can be challenging for organizations, especially those that are unfamiliar with the different types of consent, such as "deemed consent," "implied consent," and "express consent." The lack of clarity around these concepts can lead organizations to take a more conservative compliance approach and, therefore, unnecessarily rely on express consent. Therefore, the Guidelines should begin by clearly describing each of these types of consent under the ARPPIPS and the specific criteria that apply to each. More detail on "deemed consent" would be particularly helpful, given its centrality to the ARPPIPS. In addition, comprehensive guidance is needed on when to rely on "implied consent" and how to meet relevant consent criteria. "Express consent," as being the strictest type of consent, should be reserved for situations where it is warranted on the basis of the ARPPIPS and no consent exception otherwise applies. This more nuanced approach to the Guidelines would improve organizational understanding and reduce over-reliance on express consent.

Q.2 Do you think the Guidelines are legally valid? Do you think the Guidelines are internally consistent?

In our view, some of the CAI's interpretations exceed the scope of applicable legislation, and more generally go beyond the intent of the legislator.

Use of consent exceptions (para. 10). On the basis of the accountability principle set out in section 3.1 of the ARPPIPS, the CAI suggests that organizations should clearly describe any actions taken without consent in their privacy policies or other such documents.[6] Neither section 3.1—nor any other section of the ARPPIPS—provides for such an obligation. We understand that the underlying objective is to preserve individuals' rights, such as access and rectification, and to enable individuals to make a complaint if necessary. However, it does not appear that the means chosen to achieve this objective are effective. On the one hand, the inclusion of a description of all actions taken by an organization underr the ARPPIPS without consent could make privacy policies more difficult for the average individual to understand, thereby undermining their ability to exercise their rights effectively. Furthermore, given that exceptions to consent are often context-dependent and not always clearly defined in law, individuals are unlikely to be able, based on the descriptions provided in a policy, to reliably determine whether a consent exception applies in a given situation. Finally, this requirement risks diverting organizations' resources from implementing other measures that are more directly beneficial to the protection of personal information and the exercise of individual rights (e.g., setting up more effective procedures for responding to requests and complaints, training staff on their privacy obligations, improving consent mechanisms, etc.). For example, we are of the view that it is unrealistic to require that organizations describe in their privacy policies the myriad of consistent purposes for which they may use personal information that has been provided to them upon obtaining deemed consent. Consider an organization that obtains deemed consent from individuals for a financial product and then uses the customer's information for various related and consistent purposes, such as producing statements and sending monthly reminders.

Irreversibility of consent (para. 12). The CAI states that an organization that has sought an individual's consent for a particular purpose cannot, if the individual refuses or withdraws consent, reverse course and instead rely on a statutory consent exception for the same purpose.[7] This recommendation, which does not appear to be based on any specific legal requirement, fails to recognize that several consent exceptions relate to purposes that are necessary for the conclusion or performance of a contract or are otherwise required by law.[8] In other words, prohibiting organizations from processing information for purposes that benefit from a valid consent exception, ostensibly out of respect for consent, could in fact prevent the provision of a product or service to an individual, or otherwise place organizations in breach of their legal obligations. The position taken by the CAI therefore seems, in our view, to be inconsistent with section 9 of the ARPPIPS, and risks causing unnecessary and burdensome operational challenges for organizations, and particularly for small and medium-sized enterprises (SMEs). For example, many organizations have fraud detection mechanisms and models in place to protect the public and comply with their legal obligations.[9] Allowing individuals to refuse such use, on the basis of consent, would prevent organizations from detecting and reporting suspicious transactions, thereby negatively impacting all customers.

Application of the Guidelines (para. 20). Subsection 123 (9) of the *Act respecting Access to documents held by public bodies and the Protection of personal information* ("**Access Act**") sets out that the CAI is responsible for developing Guidelines to facilitate the application of the Access Act and the ARPPIPS. Despite this statutory provision, the CAI appears to ascribe a greater legal effect to the Guidelines when stating that "Organizations should make the necessary efforts to implement [the Guidelines]. If they do not, they should be able to explain why." It is our view that the CAI should limit its interventions in this respect to encouraging compliance with the Guidelines as opposed to issuing formal requirements. At the very least, the Guidelines should specify that the examples provided are for illustrative purposes only and have no legal value.

Express consent as a general rule (para. 30). The CAI states that consent must be expressed as a general rule,[10] in effect suggesting that organizations can only rely on alternative forms of consent in cases provided for by law. This interpretation seems, to our mind, to run counter to the provisions of the ARPPIPS. Indeed, subsection 12(1) of the ARPPIPS states that express consent must be obtained in order to use sensitive personal information for secondary purposes. Presumed consent is recognized in section 8.3, and deemed to be valid when individuals provide their personal information after having been adequately informed in accordance with section 8. Accordingly, in our view, it is incorrect to suggest that express consent constitutes the default form of consent insofar as presumed consent seems, to us, to encompass a wide range of situations. The CAI's position that organizations should "prioritize express consent wherever possible" deviates from privacy legislation in other jurisdictions and seems contrary to the reasonable expectations of individuals. Compliance with such a standard could lead to unnecessarily cumbersome technological processes and consent forms for processing non-sensitive personal information, and thus increase consent fatigue. In our view, the Guidelines should reflect the actual behavior of consumers, who do not have unlimited tolerance for complex notices and repeated requests for consent.

Identification, location and profiling (para. 31). The requirement set out in section 8.1 of the ARPPIPS—which requires informing individuals of the means available to activate functions that allow a person to be identified, located, or profiled—is assimilated by the CAI as being a requirement to obtain express consent.[11] According to this interpretation, the means of activation must not only be obtained through a "positive gesture," but must also meet all the other criteria for valid consent, which seems to contradict the text of the law and the general legal framework. On the one hand, section 8.1 uses the terms "means available to activate" and not "express consent." Given that the legislator took care to specify in other provisions of the law when express consent is required,[12] it seems incongruous to interpret section 8.1 as requiring such consent in the absence of clear wording to that effect. On the other hand, section 8.1 is found in Division II of the ARPPIPS, which deals with the collection of personal information, and is primarily intended to supplement the elements that must be provided to individuals under section 8 when collecting their personal information.[13] Section 8.1 is therefore first and foremost an obligation of transparency that must be read in accordance with sections 8 and following of the ARPPIPS. However, as the CAI points out, information collected in accordance with section 8 benefits from "deemed consent" under section 8.3 of the ARPPIPS, meaning that the organization is not required to assess the consent criteria set out in section 14[14]. For these reasons, it appears erroneous to equate the obligation to inform individuals of the means available to activate certain technological functions with the obligation to obtain "express consent." Rather, this obligation should be interpreted as calling for "deemed consent," based on transparency and, where available, a means of activation (e.g., checkbox, click on a button), without it being necessary to meet all consent criteria. Moreover, associating the use of identification, localization or profiling technologies to an express consent requirement is diametrically opposed to the implied consent regime for online advertising proposed by the Office of the Privacy Commissioner of Canada and to which

a large part of the Canadian industry already adheres.[15] However, we understand that the Guidelines are general in scope and may not be the most appropriate means of addressing specific concerns raised by section 8.1, particularly in relation to certain practices that may fall within its scope, such as interest-based advertising, content personalization, etc. The CAI could elaborate specific Guidelines and consult key stakeholders to formulate recommendations tailored to the technological context and the various issues related to these topics.

Information provided to individuals (paras. 49 and 50). The CAI lists information that organizations must provide to individuals in order to obtain their informed consent. While we welcome the regulator's willingness to synthesize the transparency obligation set out in statute, we believe that some nuance is necessary. First, the CAI fails to distinguish between elements which must be provided at the time of collection, and those which must be available upon request of the individual.[16] Second, neither the ARPPIPS nor the Access Act contains an obligation to inform persons concerned of "reasonably foreseeable risks or consequences associated with the activity for which consent is obtained"[17] or of "elements that may come as a surprise to the person concerned (long validity duration, use of uncommon technological means, numerous or significant risks, etc.)."[18] Rather, this requirement appears to have been borrowed from the OPC's Guidelines, and is quite difficult to interpret. Third, it should be noted that Act 25 amended the requirement contained in section 8 of the ARPPIPS (requirement to provide location where personal information is retained), with a more flexible requirement simply requiring that the possibility of information being shared outside of Quebec be mentioned.[19]

Duration of consent validity (paras. 66-69). The CAI appears to introduce an obligation for organizations to pre-determine the validity period for any consent sought, and to inform individuals of such period in order to obtain their informed consent.[20] However, the obligation to indicate the validity period for consent is not explicitly provided for in law and seems incompatible with the criterion of "informed consent."[21] The obligation to specify the validity period for consent introduces unnecessary complexity into the consent process, as in practice this period may vary depending on many factors, including the nature of the services provided, legal obligations, and the business needs of the organization. For example, an organization may obtain consent from individuals to share their personal information with a third party for the duration of the relationship between the individual and that third party, without knowing how long that relationship will last. The organization would then have to send repeated requests to individuals to extend the duration, which could disrupt their ability to obtain a product or service. In addition, it could mislead individuals by implying that their information will no longer be retained or processed after the consent period expires, when in fact the organization may be entitled to retain and process that information without their consent for a period of time. In fact, the validity period of consent and the retention period are two distinct concepts that can operate independently.[22] Finally, it should be noted that this obligation to determine the validity period for any consent sought could prove superfluous in situations where the validity period for consent is obvious to the persons concerned due to the context. Consequently, the requirement to provide such information would not necessarily contribute to more informed consent, but could rather create confusion and uncertainty for individuals.

Q.3 Is the scope of the Guidelines adequate, given their purpose (to clarify the criteria for valid consent)? Are they complete?

We would like to highlight certain ambiguities deserving of clarification in order to avoid confusion in the interpretation of the new legislative provisions.

Limitations on the right to withdraw consent (paras. 14 and 46). We believe that the CAI should seize the opportunity provided by these Guidelines to clarify the limits on the right of individuals to withdraw their consent under the ARPPIPS. In line with other Canadian privacy laws,[23] the right to withdraw consent should be subject to reasonable prior notice and reasonable contractual or legal restrictions. This interpretation appears to be consistent with the provisions of the ARPPIPS. For example, section 9 provides that requests for goods, services or employment may, in certain cases, be conditioned on the collection of information.[24] It would therefore be inappropriate to grant an absolute right to withdraw consent in these situations, as this could prevent the organization from providing the requested goods or service or fulfilling related contractual or legal obligations. Conversely, section 22 appears to establish a specific right to withdraw consent for commercial or philanthropic prospecting activities. According to general rules of statutory interpretation, the fact that this specific right is expressly stated in this particular context suggests that if the legislature had intended to create such a right to withdraw consent in other contexts, it would have done so expressly. Consequently, the absence of such an explicit statement in other sections of the ARPPIPS suggests some reasonable limitations on the right to withdraw consent may be imposed in such other contexts. In any case, clarification by the CAI on this point would contribute to a more consistent and predictable implementation of the right to withdraw consent.

Compulsory express consent (para. 31). At para. 31 (a) (ii), the CAI states that consent is not required for the use or disclosure of sensitive personal information for the primary purpose for which it is collected, while also referring to section 8.3 of the ARPPIPS which covers presumed consent.[25] Presumed consent is a valid form of consent. It must therefore be made clear that express consent is not required in the present case.

Implied consent (paras. 36-38). The notion of implied consent, as interpreted by the CAI, creates some confusion and deserves further clarification. The CAI recognizes that consent may be "implied," i.e., "inferred from the silence or inactivity of the individual or from some other action taken by the individual without a direct connection to consent," in certain situations where three conditions are met.[26] However, the CAI complicates this position by specifying that organizations must demonstrate that implied consent meets the criteria for "manifest consent,"[27] introducing uncertainty as to the precise nature of the conduct or action that would allow such consent to be inferred. In addition, the CAI specifies that implied consent must meet all of the consent criteria,[28] which presumably includes the criteria of granularity, specificity, and separateness of consent. However, the application of these criteria to implied consent raises several issues that may limit the flexibility and usefulness of implied consent. For example, it may be difficult to demonstrate the "granularity" of consent when it is inferred from the individual's silence or inactivity rather than from a clear indication. Similarly, it may not always be possible to link implied consent to a specific purpose or separate action in the absence of an affirmative statement by the individual. Finally, the CAI's position that organizations should rely on express consent "where there is doubt as to the individual's true wishes with respect to [the processing] of their information" could discourage organizations from relying on implied consent, even though it may be perfectly legitimate and appropriate in certain contexts.[29] This could lead to an increase in the number of requests for express consent, which could exacerbate consent fatigue. It would therefore be useful for the CAI to clarify its position on the notion of implied consent in order to provide clearer guidance to organizations and to ensure consistent interpretation and implementation of this notion.

Q.4 Taking into account your activities, those of the people or organizations you represent (if applicable), and your expertise, do you think these Guidelines are practical and realistic? Do you anticipate negative consequences arising from the approach proposed by the CAI in these Guidelines, and if so, what?

We would like to highlight the unrealistic nature of some of the approaches taken that may have negative repercussions on our clients.

Confidentiality incident (para. 16). First, it is our view that the provisions on confidentiality incidents (sections 3.5 to 3.8 of the ARPPIPS) should not be covered by the present Guidelines. That having been said, the CAI appears to consider that any use or disclosure of personal information without consent, and that is not otherwise subject to a consent exception, to be a confidentiality incident within the meaning of section 3.6 of the ARPPIPS.[30] As a result, in such cases, organizations must ensure to meet the obligations triggered by incidents (i.e., deploying mitigation measures, keeping of a register, notifying the CAI and persons concerned when there is risk of serious harm, etc.). While we recognize that section 3.6 of the ARPPIPS provides that "unauthorized" use and disclosure of personal information constitutes a confidentiality incident, we are of the view that such a broad interpretation of the "unauthorized" criterion risks distorting the incident reporting regime established by the National Assembly. Indeed, this approach could lead to an overabundance of entries in the organization's incident register, undermining its relevance, and to a disproportionate amount of resources being devoted to analyzing the risk of serious harm. This approach may also lead to an over-representation of confidentiality incident reports to the CAI and persons concerned, thereby trivializing the obligation of notification. In our view, the interpretation of the notion of "unauthorized" use or disclosure of personal information should not only take into account consent, but also adherence to the organization's internal policies and procedures as to the management of personal information. Moreover, it should be noted that the definition of a confidentiality incident is found in Section I.1 "Responsibilities Relating to Protection of Personal Information" of the ARPPIPS and not in Sections II and III which deal with consent rules. Moreover, it is not trivial that this definition of a confidentiality incident was introduced to the ARPPIPS in the wake of the security incident at the *Fédération des caisses Desjardins* that involved access, use and disclosure of personal information by an employee with malicious intent, and in contravention of the company's policies. In our view, the legislator intended to cover these types of situations, rather than covering *any* form of use or disclosure of personal information without consent. Since the concept of a confidentiality incident is not directly related to the rules of valid consent, and in order to avoid any confusion, we are of the opinion that this section should be removed.

Requests for repeated consent (para. 41). The CAI indicates that requesting consent repeatedly when it has already been refused may be inconsistent with its free nature; therefore, consent should only be sought once for a given purpose, unless substantial changes in context warrant otherwise. [31] While we welcome the CAI's readiness to tackle websites that incorporate certain mechanisms designed to mislead users, commonly referred to as "dark patterns," we are of the view that the CAI's position requires nuancing, given that an organization may have several legitimate reasons for reiterating a request for consent. In other words, the sole fact of repeatedly requesting consent for the same purpose should not automatically be qualified as an infringement of the voluntary character of consent without taking into account the circumstances of the request, such as the purposes pursued by the organization.

Granularity of consent (paras. 45, 59 and 60). The CAI's position on the granularity of consent criterion could create practical difficulties for organizations. According to the CAI's interpretation, this criterion would require organizations to seek consent separately for each specific purpose. In other words, they cannot combine different processing purposes in the same request for consent. In practice, however, it is not always realistic to separate each purpose of processing when requesting consent. Processing activities may be complex and involve several interdependent purposes that cannot be easily separated. For example, when an individual makes an online purchase, their email address, along with other non sensitive information, is often used for multiple, interrelated marketing activities. These activities may include customer segmentation, email marketing and retargeting on third-party platforms. Each of these purposes, while distinct, is an integral part of an overall marketing strategy based on the email address and other information collected in the course of the individual's interactions with the organization. In this context, it would be difficult, if not inappropriate, to ask for separate consent for each of these purposes. In addition, the requirement to obtain separate consent for each purpose could result in individuals having to go through multiple screens in order to access a product or service and thus significantly increase the risk of consent fatigue, an issue that the CAI itself recognizes as a problem.[32] Therefore, we believe that a more flexible approach to the granularity criterion would be appropriate, taking into account factors such as the sensitivity of the information, the reasonable expectations of individuals, and the interdependency of the purposes involved, among others.

Q.5 Are the examples provided to exemplify the CAI's guidance useful in illustrating the Commission's approach [to consent]? Are they credible?

We recognize the difficulty of the exercise of drafting clear applied examples of the criteria for valid consent given the risk of obsolescence associated with constant development of data processing technologies. We have nevertheless raised a number of issues regarding many of the examples mentioned in the present Guidelines, notably the examples describing *a priori* non-compliant practices. To avoid creating confusion among the public, we suggest that the CAI retains only examples of *a priori* compliant practices. Otherwise, to highlight the following examples, which we feel are particularly problematic:

- **Example 16.2** – This example does not consider the fact that the social network could rely on the presumed consent of users for this practice (social media platforms generally collect users' email addresses and phone numbers and use them for various purposes).The usefulness of this example is negligible since it describes a practice that targets only a very few companies (social media platforms). Subject to our previous comments (see response to question 4), it would be preferable to use a more standard example of a confidentiality incident, such as sending an email containing personal information to the wrong recipient.
- **Example 23.1** – The CAI states that the retention of an audio recording to demonstrate that consent has been obtained risks infringing the data minimization principle. However, not only is this practice recommended by other regulators[33], but it offers the most conclusive evidence of consent having been obtained. The alternative method proposed by the CAI (an agent records the date and time of consent in a file) risks creating situations of contradictory declarations (the caller claims not to have consented, contrary to what the register indicates).

- **Examples 33.1 and 33.2** – The two methods proposed to fight consent fatigue (mathematical formula and timer) are likely to have the exact opposite effect, and may generally cause irritation among consumers, negatively impacting organizations trying to achieve compliance. In both cases, the examples provided are unusual and do not reflect industry practices.
- **Example 34.1** – The example provided gives the impression that express consent is required for any project involving an artificial intelligence system, even when the personal information involved is not sensitive. Indeed, no details are provided regarding the PIA conducted by the Access to Information and Privacy Committee. Moreover, it is unclear why the organization did not instead rely on a consent exception (e.g., compatible purpose or research purpose) for such use. This example risks stifling innovation as it would unreasonably restrict AI work to offer a better consumer experience.
- **Example 34.2** – This example concludes, quite hastily, that cookies are a means of profiling and are thus subject to section 8.1 of the ARPPIPS. It is not clear, however, whether the customization (profiling) described in this example is performed by the cookies or by the company's internal recommendation algorithms. In addition, section 8.1 does not set out that "Accept" and "Reject" buttons must be displayed in the same manner, and this section is not subject to the criteria for valid consent under section 14. Nor does section 8.1, as it is worded, provide for any requirement of express consent, or even consent more generally. In our view, it would be preferable to have an example of a situation that clearly requires express consent (e.g., disclosure of sensitive personal information to a third party).
- **Implied Consent** – All the examples proposed (36.1 to 36.4) describe *a priori* non-compliant practices. Instead, it would be useful to have examples of practices that are consistent with implied consent given the uncertainty surrounding this notion (see our response to question 3).
- **Example 42.2** – This example conflicts with Canada's Anti-Spam Legislation, which provides that an organization may send commercial electronic messages to a recipient on the basis of implied consent where the recipient has an ongoing business relationship with the individual.[34] We believe it would be preferable to use an example that does not involve commercial electronic messages to avoid any confusion with Canada's Anti-Spam Legislation, as well as section 22 of the ARPPIPS (e.g. sending promotional offers through paper brochures).
- **Example 46.2** – This example is confusing: it describes a service that does not exist in the market to our knowledge. Indeed, personalization is nowadays an essential aspect of any digital platform, whether it's a social network, a news platform, or a streaming service. Thus, this functionality may, in some cases, be considered "essential" for the provision of the service. In any case, "eight clicks" seems, to us, to be an arbitrary standard for determining how difficult it is to withdraw one's consent to a particular feature of a digital platform. It seems only natural that withdrawing consent after joining a platform requires more steps than providing consent at the time of joining. In short, we suggest avoiding the mention of a specific number of clicks.
- **Example 57.2** – This example is confusing, as the transfer of customer contact information to a new business partner could be covered by the consent exception for a commercial transaction.[35] Moreover, this example neglects to consider the fact that the law allows organizations to inform individuals of the categories of third parties to whom the information may be communicated (art. 8 para. 2 ARPPIPS). Thus, the organization may have had valid presumed consent for such disclosure.

- **Example 63.1** – This example makes an association between the clear language requirement of the consent request (art. 14 para. 1 ARPPIPS) and obtaining express consent via a checkbox. However, there is no indication in the proposed situation that express consent is required by law. The example should be limited to a rewording of the consent request in clear language.
- **Example 67.1** – This example refers to an "obligation" to inform individuals of the period of validity of their consent. However, this obligation does not exist in the law (see our reply to question 2). We believe that the example provided should not focus on the obligation of transparency, as the latter is not related to the temporary nature of consent.
- **Example 71.1** – This example is confusing, as the disclosure of the insured's personal information to the insurer seems, to us, to be a primary purpose that would be covered by presumed consent. Moreover, the addition of the "Yes" / "No" boxes seems redundant to us, given that this example deals with the distinct nature of consent and not with the form of consent.

Q.6 Is the format of the Guidelines adequate and easy to consult? Is the text clear?

A number of our clients have indicated that reviewing the Guidelines in their entirety in a single sitting was difficult given the length of the document. We suggest shortening the document to make it easier for readers to fully understand. First, it would be more efficient, in our view, to have one document for the public sector and one for the private sector. Combining the two regimes makes the document unnecessarily long and complex. This way, the CAI could remove repetition throughout the document (some of the validity criteria, notably granularity, are interpreted differently in several sections, thus creating confusion) as well as the number of examples provided (see our response to question 5).

Endnotes

1 *Act respecting access to documents held by public bodies and the Protection of personal information*, RSQ, c. A-2.1 ("**Access Act**").

2 *Act respecting the protection of personal information in the private sector*, RSQ, c. P-39.1 ("**ARPPIPS**").

3 On this subject, we recommend the following articles: Colin M Gray and al., "Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective" (2021) in Proc 2021 CHI Conf Hum Factors Comput Syst (New York: Association for Computing Machinery) 1 on pages 6 to 8, Neil Richards & Woodrow Hartzog, "The Pathologies of Digital Consent" (2019) in 96:6 Wash ULR 1461 on pages 1492 to 1494; Bart W. Schermer and al., "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection" (2014) in 16 Ethics Inf Technol 171 on pages 176 to 178 and Hanbyul Choi and al., "The role of privacy fatigue in online privacy behavior" (2018) in 81 Computers in Human Behavior 42 on page 43.

4 Commission d'accès à l'information, *(2023-1) Guidelines on the Criteria for Valid Consent*, May 16, 2023, para. 33 ("**Guidelines**").

5 It is worth noting that the European Commission has recently identified several challenges with the excessive use of banners on websites, which not only disrupt the web experience, but are often ignored by users (see "Cookie Pledge: A reflection on how to better empower consumers to make effective choices regarding tracking-based advertising models" available at: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en).

6 Guidelines, para. 10.

7 Guidelines, para. 12.

8 Section 12 of ARPPIPS provides that personal information may be used within the enterprise for purposes other than those for which it was collected, without the consent of the individual, "if its use is necessary for the purpose of providing or delivering a product or providing a service requested by the person concerned" (s. 12 (2) (4) ARPPIPS). Section 18 ARPPIPS which provides that a person who carries on a business may, without the consent of the person concerned, disclose personal information that he holds about others "to the Director of Criminal and Penal Prosecutions if the information is required for the purposes of the prosecution of an offence under an Act applicable in Québec" (s. 18 (2) ARPPIPS); "to a person or body responsible, by law, for the prevention, detection or repression of crime or statutory offences who requires it in the performance of his duties, if the information is needed for the prosecution of an offence under an Act applicable in Québec" (s. 18) (3) ARPPIPS); "to a person to whom it is necessary to communicate the information under an Act applicable in Québec or under a collective agreement" (s. 18 (4) ARPPIPS) and "to a person or body having the power to compel communication of the information if he or it requires it in the exercise of his or its duties or functions" (s. 18 (6) ARPPIPS).

9 Notably the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17.

10 Title 2.1.1 and para. 30.

11 Guidelines, para. 31 (b).

12 Section 12 and of 13 ARPPIPS and section 44 of the *Act to establish a legal framework for information technology*.

13 Section 8.1 of ARPPIPS specifies that it applies "[i]n addition to the information that must be provided in accordance with section 8."

14 Guidelines, para. 14.

15 OPC, *Policy position on online behavioral advertising* (Revised August 13, 2021), https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/bg_ba_1206/

16 Organizations shall only be obliged to provide the elements provided for in subparagraphs (f) and (g) of paragraph 49 if requested by the individual.

17 Guidelines, para. 49 (i).

18 Guidelines, para. 50(a)(1)

19 Guidelines, para. 49 k). Former s. 8 (3) ARPPIPS (prior to the coming into force of Law 25) " A person who collects personal information from the person concerned must, when establishing a file on that person, inform him... of the place where the file will be kept and of the rights of access and rectification. New s. 8 (2) ARPPIPS (after the coming into force of Law 25): "Where appropriate, the person concerned shall be informed ... of the possibility that the information may be disclosed outside Quebec". Former s. 65 (1) of the Access Act (prior to the coming into force of the Law 25): "Every person who, on behalf of a public body, verbally collects personal information from the person concerned shall name himself or herself and, at the time of the first collection of information and subsequently upon request, inform him or her of the name and address of the public body on whose behalf the information is collected...". New s. 65 para. 2 of the Access Act (after the coming into force of Law 25): "Where appropriate, the person concerned shall be informed ... of the possibility that the information may be communicated outside Quebec."

20 Guidelines, para. 68.

21 The purpose of this criterion is to enable individuals to understand the nature, purpose and consequences of the collection, use or disclosure of their personal information, and to make informed decisions about how their personal information is handled.

22 See section 23 ARPPIPS, which states that an organization must destroy or anonymize personal information in its possession once the purposes for which the information was collected or used have been fulfilled, subject to applicable statutory retention periods.

23 Principle 4.3.8 of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"); sections 9 and 35 of the Personal Information Protection Act (British Columbia); sections 9 and 35 of the *Personal Information Protection Act* (Alberta).

24 Section 9 of ARPPIPS: (1) collection is necessary for the conclusion or performance of a contract; (2) collection is authorized by law; (3) there are reasonable grounds to believe that the request is not lawful.

25 Guidelines, para. 31 (a) (ii).

26 Guidelines, para. 36. Implied consent may be relied upon where the processing activity for which consent is sought: (i) does not involve sensitive personal information; (ii) does not fall outside the reasonable expectations of the individuals concerned; and (iii) no risk of serious injury arises from the processing activity.

27 Guidelines, para. 37.

28 Guidelines, para. 38.

29 Guidelines, para. 39.

30 Guidelines, para. 16.

31 Guidelines, para. 41 (b).

32 Guideline, para. 33.

33 The CRTC has indicated that a complete and unedited audio recording of the consent given constitutes adequate evidence of oral consent under Canada's Anti-Spam Legislation (see *Compliance and Enforcement Information Bulletin CRTC 2012-548*, para. 23).

34 Section 10 Canada's Anti-Spam Legislation.

35 Section 18.4 ARPPIPS.