Notice of Consultation

May 16, 2023

Guidelines 2023-1 on Criteria for Valid Consent

Context and objective

The *Commission d'accès à l'information* (CAI) oversees the application of Quebec's main privacy laws, the *Access Act* and the *Private Sector Act* (see updated administrative versions on its website [*in French only*]). The CAI has the function of developing guidelines to facilitate their application. In light of the upcoming coming into force of the substantive portion of Bill 25, which amends these Acts, the CAI has prepared initial guidelines on the criteria for valid consent based on the Acts as they will be in force on September 22, 2023.

These guidelines, which are set out on page 4 of this document, are intended to assist organizations and individuals subject to these Acts to better understand the relevant elements for assessing each statutory criterion for valid consent (*Access Act*, s. 53.1; *Privacy Act*, s. 14). The guidelines are illustrated with examples. The guidelines are not intended for the health sector.[1]

Consultation

The CAI is holding a six-week consultation, ending June 25, 2023 at 11:55 p.m., to obtain comments on the text of the guidelines. In addition, the CAI wishes to explore the need for future guidelines, both in the areas of access to information and privacy.

The consultation has two components, depending on the audience:

1. **General public, persons and organizations subject to the Acts**: a questionnaire is available on the Consultation Québec platform [*in French only*]. It allows brief comments on the proposed text and to formulate suggestions for future guidelines.

2. **Stakeholders previously targeted**: 18 stakeholders targeted by the CAI for their expertise, their representativeness or the importance of their activities have agreed to submit a brief on the guidelines. Instructions will be sent to them by email. The list of stakeholders is provided below on page 3. Submissions will be made public at the end of the consultation period.

One of the reasons the CAI is conducting a mixed consultation, part of which is by invitation, is to respect its organizational capacity to analyze comments. The CAI's goal is to make the final version of its guidelines available in a timely manner so that organizations can benefit from them as soon as possible.

---

[1] The provisions of the *Act respecting health information and social services and amending various legislative provisions*, which governs health information, are not included in the scope of the guidelines, as it will be a separate framework.

Analysis of comments and feedback

The CAI is committed to analyzing the comments received in a serious and rigorous manner. It reserves the right to reject all or part of the comments if they are not relevant to the subject of the consultation. By September 2023, the CAI will prepare a feedback document outlining the key comments received and respond to them.

The CAI's consultation is separate from any other jurisdictional, oversight or other activities it conducts. Comments received during the consultation will be used only to improve the guidelines. For example, they will not be used in investigations.

Influence of the process

Comments received will be used to adjust the text as needed. Examples, level of detail and format of the text will be modified. The CAI's overall direction for the sections of the Acts is less likely to change and will be modified only if the comments reveal new elements in the analysis.

The CAI intends to release the final text of the guidelines in October 2023. This date may change depending on the volume of comments received and the changes to be made.

Limitations of the consultation

The CAI:

- **Will not provide individualized responses** to questions about legislation submitted during this consultation;
- **Will not process any submissions that have not been received by invitation**. However, there is an opportunity to become a targeted stakeholder at a future consultation. There is a section of the questionnaire for organizations to request this.
    - The CAI invites you to contact some of the stakeholders listed below (e.g., sector representatives) if you would like to share your views on the guidelines or possibly partner with them to produce the brief;
- **Does not commit to action on the proposed guideline topics** but will consider them in planning its future work.

Protection of personal information

Information concerning the collection of personal information by the CAI in the context of the consultation is available on the Consultation Québec platform [*in French only*].

Questions about the consultation

For any additional information, please contact Mr. Xavier St-Gelais at xavier.st-gelais@cai.gouv.qc.ca or by phone at 418 528-7741, extension 51113.

List of stakeholders who will file a brief

1. Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité
2. Ministère de la Santé et des Services sociaux
3. Barreau du Québec
4. Fédération des centres de services scolaires du Québec
5. Fonds de recherche du Québec
6. Association des professionnels en accès à l'information et en protection de la vie privée (AAPI)
7. Fasken Martineau DuMoulin, LLP
8. Border Ladner Gervais, LLP
9. Gowling WLG (Canada), LLP
10. Lavery de Billy, LLP
11. Fédération des chambres de commerce du Québec
12. Conseil du patronat du Québec
13. Association canadienne des compagnies d'assurance de personnes
14. Association des banquiers canadiens
15. Association canadienne du marketing
16. Observatoire international sur les impacts sociétaux de l'IA et du numérique
17. Option consommateurs
18. Ligue des droits et libertés

Guidelines 2023-1

Consent: Criteria for Validity

Act respecting Access to documents held by public bodies and the Protection of personal information, section 53.1

Act respecting the protection of personal information in the private sector, section 14

(The text is based on these laws as they will be in force on September 22, 2023)

Version 0.1 - Document for consultation

(Warning: These guidelines are not yet in force)

Release date: May 16, 2023
Revision date: [No revision]

TABLE OF CONTENTS

1. INTRODUCTION

1. Legal basis. The Commission d'accès à l'information (hereinafter the "CAI") has developed these guidelines in accordance with section 123 of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (hereinafter the "*Access Act*").

2. Objective. The CAI is issuing these guidelines to facilitate the understanding of the criteria for valid consent that public and private organizations (hereinafter referred to as "organizations"[2]) must obtain from an individual concerned with personal information. These criteria are provided for:

a. In the *Access Act*, at section 53.1;

b. In the *Act respecting the protection of personal information in the private sector* (hereinafter the "*Private Sector Act*"), at section 14.

In this document, unless other sections are explicitly mentioned, the guidelines are intended to construe these two sections.

3. Exclusions. These guidelines do not address consent to disclosure of information that is not personal – such as technical, financial or trade secret information (*Access Act*, ss. 23, 24, 25 and 49).

They are also not intended to provide specific guidance on when consent is or is not required, except for the general information provided in section 1.1. They focus on the criteria to be met when consent is indeed required by law.

4. Legal references. These guidelines are based on the *Access Act* and the *Private Sector Act* as amended by the *Act to modernize legislative provisions as regards the protection of personal information* (SQ 2021, c 25, or Bill 25). The CAI makes available administrative versions of the *Access Act* and the *Private Sector Act* incorporating the Bill 25 amendments [*in French only*].

5. Examples. The examples given in these guidelines are fictitious but may be based on actual practices. They are simplified to highlight specific consent issues and thus illustrate a specific aspect of the text (e.g., a single criterion of validity). Most often, examples are associated with one sector (public or private), but some apply to both. A single example will sometimes accompany a paragraph when the CAI considers that it illustrates its meaning for all sectors.

6. Other legislation. Organizations are responsible for knowing and complying with their consent obligations under other sectoral legislation, such as the *Act respecting health services and social services* (CQLR, c S-4.2), or general legislation, such as the *Civil Code of Québec* (CQLR, c CCQ-1991). Furthermore, obtaining valid consent does not negate other legal obligations of organizations with respect to the protection of personal information.

[2] The term "organization" also includes individual companies in the context of these guidelines.

1.1. Consent is central to the principle of control by individuals over their personal information

7. The concept of consent. By default, personal information is confidential. Individuals can exercise control over the use and circulation of their information through consent. Consent, which is related to personal autonomy, implies that individuals agree to what happens to their information. Consent is an important concept in Quebec privacy legislation.

In order to be in compliance with the law and thus be valid, consent must meet certain criteria. These guidelines focus on how to meet each of these criteria.

8. General rule. While these guidelines are not intended to set out the exact situations in which consent is or is not required, legislation generally requires organizations to obtain valid consent, including, but not limited to, the following situations:

a. To collect personal information from and relating to a minor under the age of 14 (*Access Act*, s. 64.1; *Private Sector Act*, s. 4.1) – consent is given by the parent or tutor;

b. To collect, personal information from a third party in the private sector (*Private Sector Ac*t, s. 6);

c. To use personal information for a secondary purpose, i.e., for a purpose other than that for which it was collected (referred to as the primary purpose) (*Access Act*, s. 65.1; *Private Sector Act*, s. 12); and

d. To communicate or disclose personal information to a third party (*Access Act*, ss. 53, 59 and 88; *Private Sector Act*, ss. 13 and 40).

In addition to allowing the individual to give permission to the organization, the consent request also serves a transparency purpose. It is one of the elements that informs the individual of what the organization intends to do with his or her personal information.

9. Exceptions. In some cases, the *Access Ac*t and the *Private Sector Act* provide exceptions that allow an organization to use or communicate personal information without obtaining consent. Many other statutes also provide similar exceptions. Where an exception applies, since there is no consent, the validity criteria are not relevant.

10. Use of exemptions. Under the accountability principle (*Access Act*, s. 52.2; *Private Sector Act*, s. 3.1; see Section 1.3), an organization must be able to demonstrate that an exception allows it to use or communicate personal information without consent. It must also be transparent.

The organization should clearly describe its non-consensual actions in a privacy policy or other similar documents. In this way, individuals are informed of how their information is used and communicated by the organization, thereby safeguarding their rights to access, rectify, de-index and complain to the organization or to the CAI, etc. To exercise these rights, one must be adequately informed.

11. Optional nature of exceptions. However, most exceptions are optional. Organizations are not obliged to use them and may therefore choose to rely on consent instead, particularly where there are no practical difficulties in obtaining it (e.g., small number of individuals involved, easy to reach, non-emergency situation).

Depending on the context, consent may sometimes be more advantageous to the organization, for example to facilitate demonstrability of compliance with the law (see Section 1.3). Importantly, consent can also be withdrawn later by the individual concerned (see Section 2.2), which adds a means of control over his or her personal information, in addition to the rights mentioned above. This may be part of the organization's analysis when determining whether or not to rely on exceptions to consent for certain activities.

12. Irreversibility. If, for a specific purpose, an organization chooses to rely on consent rather than an applicable exception for the collection, use or communication of personal information, it must respect the choice of the individual concerned. Thus, the organization cannot, for that same purpose, take a step back and choose to rely on that exception if these individuals refuse to consent or withdraw their consent. To do otherwise would render consent meaningless as a means of control.

13. Cases of doubt. If an organization is unsure or cannot demonstrate that an exception applies in a given situation, it should instead obtain valid consent from the individual concerned.

14. Presumed consent. When an individual provides his or her personal information after having received the statutory information (*Access Act*, s. 65; *Private Sector Act*, s. 8), he or she is presumed to consent to its use and communication for the purposes for which it was collected and of which he or she is aware (*Access Act*, s. 65.0.2; *Private Sector Act*, s. 8.3).

This presumed consent implies that the organization is not required to assess its validity criteria. However, the individual concerned may subsequently withdraw consent.

15. Consent and necessity. At all stages of the life cycle of personal information, i.e., collection, use, communication, storage and destruction, the legislation places a limit on the necessity for the information to accomplish the purpose (e.g., *Access Act*, ss. 64, 65.1, 67; *Private Sector Act*, ss. 5, 12, 18).

Consent can never override this requirement. Therefore, consent alone is not sufficient to authorize an operation involving personal information.

[A priori non-compliant practice]

Example 15.1 – At its general meeting, an association of sixteen co-owners adopts a unanimous resolution to install surveillance cameras capturing images in all the corridors of a condominium building in order to ensure the security of the premises. However, there is no history of significant security problems. The cameras purchased are positioned at an angle to capture the front door of each unit.

Despite the unanimous agreement of the co-owners, which indicates their consent, the fact of capturing images throughout the building is likely, with respect not only to the co-owners but also their guests, an invasion of privacy whose

impact is not proportional to the security objective pursued. Indeed, people have an expectation of privacy when they are on residential premises; however, the angle of the cameras means that they record and document their comings and goings, the people they meet, etc. Furthermore, the security problem is theoretical and not proven since no previous incidents have occurred. **In these circumstances, the association's collection of videotapes does not meet the necessity test, and consent is not sufficient to bring it into compliance with the law.**

16. Confidentiality incident. Accessing, using or communicating personal information without the consent of the individual to whom the information relates, when required by law, constitutes a confidentiality incident (*Access Act*, s. 63.9; *Private Sector Act*, s. 3.6). If an organization detects a problem related to the failure to obtain valid consent, it must comply with its incident-related obligations (keeping a record, notifying the CAI and the individuals concerned if there is a risk of serious injury, etc.).

[A priori non-compliant practice]

Example 16.1 – Employees of a municipality provide their banking information to the human resources department when they are hired in order to receive their salaries. In the course of organizing a holiday event, two employees in the department use this banking information to send an electronic fund transfer request to those who have confirmed their attendance at the event and are required to pay their registration. **This secondary use is not authorized by any statutory exception and the employees did not consent to it. This is a confidentiality incident for the municipality. The municipality must record it in its registry and assess the risk of serious injury to the individuals concerned to determine whether it should notify them and the CAI.**

[A priori non-compliant practice]

Example 16.2 – A social network is offering users the ability to enhance their account security by adding an email address or phone number for multi-factor authentication. This information is stored in the user's profile. At the same time, the network offers external publishers the opportunity to serve ads to users who are already on their own customer lists. To do this, the publishers upload their list, in encrypted format, to the social network tool, and the algorithm verifies whether the customers are users based on different information. In particular, it takes into account the phone number and email address contained in the users' profile, which it compares to those of the marketing lists. **In doing so, the social network is using this personal information without authorization, since it has not obtained the consent of the individuals concerned, even though no exceptions apply (compatible purposes, security reasons, application of a law, clear benefit to the individual, etc.). This is a confidentiality incident.**

1.2 These guidelines represent the expectations of the CAI

17. Individuals concerned. These guidelines are specifically intended for the following individuals within an organization:

a. The individual with the highest authority;

b. The individual accountable for the protection of personal information;

c. Members of the Access to Information and Privacy Committee, in the public sector;

d. Personnel who work in protection of personal information, service design or information technology;

e. Personnel who collect consent related to personal information.

18. Intention of the CAI. These guidelines represent the CAI's expectations of organizations with respect to obtaining valid and meaningful consent. The additional detail provided in the guidelines is intended to assist in the enforcement of the law.

19. Authority of the guidelines. These guidelines are more important than the CAI's guidance documents, but they do not have the force of law. Laws and regulations take precedence at all times over their content.

20. Application. In carrying out its oversight functions, the CAI will consider compliance with these guidelines. Organizations should make every effort to enforce these guidelines. If they do not, they should be able to explain why.

21. Evolution. These guidelines may be modified in the future and others, more focused on certain sectors of activity, for example, may complement them.

1.3. Organizations must be able to demonstrate their compliance

22. Accountability. Organizations are responsible for protecting the personal information they hold (*Access Act*, s. 52.2; *Private Sector Act*, s. 3.1). They must be able to demonstrate that they are complying with their statutory obligations (principle of demonstrability), including obtaining consent and ensuring its validity.

23. Method of documenting that consent was obtained. In these guidelines, the CAI does not prescribe a method for proving that consent has been obtained. Organizations should develop methods appropriate to their own context and activities. However, they should always minimize the collection of personal information: documenting proof of consent should not require the collection of more information than is necessary, depending on the context.

[A priori non-compliant practice]

Example 23.1 – To document that consent was obtained for the communication of certain tax information to a third party, a ministry decides to retain audio recordings of entire telephone conversations during which the individuals concerned give consent to an agent. **This method is likely to fail to respect the minimization principle**, as it

results in the collection of additional information (audio recording, full conversation) only to demonstrate compliance. Instead, the ministry could make a note in a file of the date and time of the consent, as well as the name of the staff member who collected it.

[A priori non-compliant practice]

Example 23.2 – An insurance company wishes to document its obligation to obtain consent for the communication of indemnification information to a third party. Through its web form, it decides to record the users' cursor movement pattern on the consent page, from the time it is opened to the time they check the "I consent" box, to show that the action comes from them and is thoughtful. It also records the duration of the operation. **This method is likely to fail to respect the minimization principle**, as it involves the collection of additional information (mouse usage pattern, length of time on the page) only to demonstrate compliance. Instead, the insurance company could record only the checked status of the box, along with the date and time of the operation, in the users' file.

24. Documentation of the validity of consent. In addition to documenting that consent was obtained, organizations must be able to demonstrate its validity. Again, it is up to organizations to determine the best method for doing so. This method may involve, for example, keeping factual elements related to the request of consent (information given in advance, the action taken to consent and what differentiates it from other actions taken, etc.), including a history of these elements demonstrating that the obligation was fulfilled at a previous date.

[A priori compliant practice]

Example 24.1 – A government corporation providing digital services keeps an archive with screenshots of its online consent form. Each is accompanied by an indication of the time period it represents. Each time a change is made to the form, the government corporation adds a new screenshot to its archive. This practice allows the government corporation to keep a record of the elements allowing an assessment of the validity of a consent obtained at an earlier period, particularly in the context of an inspection.

[A priori compliant practice]

Example 24.2 – A company operating a call centre has a policy and procedures relating to customer consent for the communication of personal information. One of the procedures, which sets out a framework for service requests, has been updated three times in recent years. On each occasion, the company retained a copy of the previous versions. **This makes it easier for the company to demonstrate that consent obtained under a previous version of the procedure was informed, for example.**

25. Authentication of the individual concerned. Since consent is an expression of personal will, an organization must ensure that it obtains consent from the individual concerned (or his or her legal representative, if applicable). In doing so, the organization should aim for a degree of certainty that is reasonable in the context of its activities. When there is a legal representative, the organization should also verify the status of the person giving consent (parental authority, beneficiary, representative, etc.), always aiming for a reasonable degree of certainty. This verification may be accomplished by validating certain personal information, but the organization must not retain or collect more information than is necessary.

26. Timing of consent. An organization must generally obtain consent before performing the actions authorized by consent.

2. CRITERIA FOR VALID CONSENT

27. Criteria. Valid consent is defined in Section 53.1 of the *Access Act* and Section 14 of the *Private Sector Act*, which contain eight criteria (each box in the text is a link to a specific section of these guidelines):

> *"Consent [under the law] must be **clear**, **free** and **informed**, and must be **given for specific purposes**. It must be **requested for each such purpose**, in **clear and simple language**. **If the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned. When requested by the person concerned, assistance must be provided to help the person concerned understand the scope of the consent requested.***
>
> *[…]*
>
> *Consent is **valid only for the length of time needed to achieve the purposes for which it was requested**.*
>
> *Consent given otherwise than in accordance with [the law] is without effect."*

28. Interrelationship between criteria and importance of each of criterion. The criteria are interrelated. They are all important: if one criterion is not met, the consent is not valid and has no effect. The first four (clear, free, informed, specific) are fundamental, while the next four (granular, understandable, temporary, distinct) relate to particular aspects of the first four and ensure full validity. For example, a consent must be presented in simple and clear terms to be informed and specific. Throughout the text, the relationships between the criteria are clarified.

2.1. Consent must be clear

29. Clear. A consent must first be clear, that is, obvious, and given in a way that demonstrates the real will of the person concerned. In most cases, this will should be express, or explicit, but it may be implicit in certain circumstances.

2.1.1. In general, consent must be express (explicit)

30. Priority to express consent. Consent is express (or explicit) when the person makes an active gesture (or makes a statement) that clearly indicates his or her agreement. This gesture or statement serves no other purpose than to consent and is said to be positive: it indicates acceptance, not refusal. There is then no doubt as to the real will of the person. The English expression *opt in* also designates this form of consent.

An organization should give priority to express consent whenever possible.

31. Mandatory express consent. In some situations, the organization is required to obtain express consent. For example:

a. **Sensitive information:** The use or communication of sensitive information must be authorized by express consent (*Access Act*, ss. 59 and 65.1; *Private Sector Act*, ss. 12 and 13).

   i. Sensitive information is information that is medical, biometric[3] or otherwise intimate in nature, or information whose context of use or communication gives rise to a high reasonable expectation of privacy (*Access Act*, s. 59; *Private Sector Act*, s. 12);

   ii. Consent is not required for the use or communication of sensitive information for the primary purpose for which it was collected (*Access Act*, s. 65.0.2; *Private Sector Act*, s. 8.3) or where exceptions to consent apply.

b. **Identification, location and profiling:** The legislation requires that technologies allowing the person concerned to be identified, located or profiled be turned off by default; organizations must inform individuals of the means to activate them (*Access Act*, s. 65.0.1; *Private Sector Act*, s. 8.1). This amounts to a requirement for express consent.

[A priori compliant practice]

Example 31.1 – An organization that provides allowances to people with disabilities has sensitive information about their health and financial situation. As part of an evaluation of one of its programs, the organization appoints an employee to study the effectiveness of the allowance, including client satisfaction. At the time of collecting the information to provide the allowance, the organization made no mention of using it for evaluation purposes. In order to allow the evaluator to use the information of the 275 individuals who received the allowance, the organization must therefore obtain their express consent since the information is sensitive. **To ensure that this consent is unambiguous, the organization develops a self-supporting form and sends it to the individuals to sign.**

[A priori compliant practice]

Example 31.2 – A dating application allows its users to determine a larger or smaller area around their location to filter potential partners based on their proximity. In order to access this feature, users must activate geolocation on their mobile device. **The application informs them that the feature relies on the collection of GPS geolocation data and provides them with the various information required to comply with the law. It then explicitly asks them for permission to enable geolocation.**

[3] In this regard, the *Act to establish a legal framework for information technology* (CQLR, c C-1.1, s. 44) also requires that the express consent of the person concerned be obtained before requiring that the verification or confirmation of his or her identity be made by means of biometric characteristics or measurements.

[A priori non-compliant practice]

Example 31.3 – A government corporation needs to produce statistics on the diversity (gender, ethnic, linguistic, etc.) of its personnel to create an action plan against discrimination. Without access to information on the sexual orientation of employees, the human resources team is considering using information on the gender of the employee's dependent spouse from each employee's group insurance form to calculate the proportion of personnel with a same-sex spouse. **In these circumstances, it must ensure that it obtains the express consent of the employees since the sex of their spouse is sensitive information: it is very likely to reveal their sexual orientation, information that is protected by the *Quebec Charter of Rights and Freedoms*.**

[A priori non-compliant practice]

Example 31.4 – A massage therapy clinic organizes a series of health and wellness conferences in collaboration with other health care providers. The owner wishes to send personalized invitations to her clients. She plans to use the data on their health status and medical history, collected during the opening of their file to ensure that the treatments offered are safe, to invite them to attend conferences relevant to their situation. **This secondary use of sensitive (medical) information cannot be done without express consent.** Since she had not sought such consent beforehand, the clinic owner finally decides to announce the conferences in the clinic's newsletter already sent to clients who have agreed to receive news about events.

[A priori compliant practice]

Example 31.5 – After a series of attempted break-ins, an explosives manufacturing company wants to tighten access control to its reagent storage site to limit it to authorized personnel only. The company is considering the purchase of a biometric hand shape recognition system. After conducting a privacy impact assessment that takes into account the context of its activities, the company concludes that its situation justifies the use of this technology. Since the system relies on biometric characteristics, **the company acknowledges that it needs express consent and develops a consent form for the collection and use of these characteristics for the authentication of authorized personnel. Employees who wish to do so can sign the form and those who do not can opt for an electronic access card system.**

32. Method of obtaining the consent. An organization is free to develop express consent mechanisms that are appropriate to its activities, as long as they comply with the law. These mechanisms should be tailored to the individuals concerned, the context and the type of interface used. Signing a document, activating a box or answering a question in the affirmative are all ways of providing express consent (active, positive and unequivocal gestures), but they are not the only options available.

[A priori compliant practice]

Example 32.1 – An employee of a public body provides services to people with mobility impairments, the majority of whom cannot write or use touch screens. In order to validate financial aid, he must share information about their case with a ministry. His organization's governance rules preclude the use of exceptions to consent where it is, in practice, easy to obtain (e.g., where a small number of individuals are concerned). The employee must therefore rely on the consent of the individuals concerned for the communication of the information. The employee asks for consent verbally and records the date, time and details of the consent in the file notes to meet the obligation of **demonstrability. This mechanism allows for a clear consent (explicit, in this case) to be obtained, taking into account the particularities of the clientele for whom the**

to be obtained, taking into account the particularities of the clientele for whom the services are being provided. ***[A priori compliant practice]***

Example 32.2 – A manufacturer markets an educational connected toy aimed at children aged 5 to 8. The toy records the child's first name and measures the progress of the child's answers to questions related to letters and numbers from week to week (correct or incorrect answers, response time, etc.). These results are available on a secure web portal for parents. The manufacturer must obtain parental consent to collect this information from children. When the toy is set up, it provides auditory instructions to parents. To consent to the collection of the child's progress information, they are asked to press three coloured buttons on the front of the toy simultaneously. **This mechanism allows for a clear consent (explicit, in this case) to be obtained, taking into account the device with which the parents are interacting.**

33. Consent fatigue. Depending on the context of its activities, an organization should take steps to mitigate consent fatigue. Indeed, every day, we are all asked to give consent in a multitude of contexts. In the digital world, this is often done by checking a box or clicking a button. Although the repetitive nature of these gestures can make them meaningless, it is important that the person concerned be aware that he or she is giving consent, particularly so that he or she understands the information made available to him or her (informed consent criterion; see Section 2.3).

[A priori compliant practice]

Example 33.1 – An organization offers an application to access all of its services. The nature of the organization's activities means that individuals frequently interact with this application. As a result, the organization often collects consents. It asks users to confirm the consents by answering a mathematical question (such as 8 + 4). **This helps to "break the rhythm" and partly combats consent fatigue.**

[A priori compliant practice]

Example 33.2 – A bank's application frequently seeks consent from its customers to disclose their personal information. When it needs to, it displays, on a random basis, a pop-up window with simple, clear information and a button to consent. The window is displayed for one minute, with a countdown timer, to give customers enough time to review the information and the request being made. The accept or decline consent buttons do not activate until the time limit has passed. **By doing so, the bank "breaks the rhythm" and partly combats consent fatigue.**

34. Inadequate methods. Even taking into account consent fatigue, an organization cannot *presume* express consent: this must involve an active and positive (unequivocal) gesture. The following methods of obtaining consent are therefore not valid since they do not ascertain beyond doubt the will of the individual concerned:

a. Use of already checked boxes;
b. Simple possibility of subsequent refusal (*opt out*);
c. Deduction based on the silence or the inactivity of the individual;
d. Deduction based on another gesture made by the individual.

All of these methods are associated with implied consent (see Section 2.1.2).

[A priori non-compliant practice]

Example 34.1 – In order to respond more effectively to requests from individuals, an organization wants to develop an artificial intelligence system (AIS) to prioritize cases. It plans to develop the AIS using data concerning the use of its services over the past three years. After conducting a privacy impact assessment, its Access to Information and Privacy Committee determined that express consent was required to use the information for this new purpose. Despite this conclusion, the organization decides to send an email to the individuals concerned informing them of this new use, noting that they may contact the organization's Privacy Officer to withdraw their consent to this use. **Since the organization presumes consent and does not offer the opportunity to affirmatively opt in, it does not obtain express consent.** It could have done so, for example, by asking individuals to confirm their consent through a personalized web link linked to their file.

[A priori compliant practice]

Example 34.2 – A magazine's website provides personalized article recommendations based on readers' interests, inferred by an artificial intelligence algorithm. The information used for inference (pages viewed, clicks, browser language, time spent on each page, etc.) is collected using cookies placed on the reader's device. Since this technology allows for profiling, the magazine displays a pop-up window during the first visit of the site and provides the individuals concerned with the information required by the *Private Sector Act* (notably, ss. 8 and 8.1). They then have the option of accepting or refusing the deposit of cookies for the purpose of personalizing recommendations. To do so, two clearly identified buttons ("*Accept*" / "*Refuse*"), highlighted in the same way, appear at the bottom of the pop-up window. **This allows the magazine to obtain express consent.**

35. Risk of confusing the intentions of the individual concerned. For consent to be express, an organization must avoid confusing it with another gesture made by the individual, such as confirming that the terms of conditions have been read. It must design consent mechanisms that are clear to the individuals concerned. This is related to the distinctiveness of consent (see Section 2.8).

2.1.2. In some situations, consent can be implicit

36. Possibility of implicit consent. In certain circumstances, the form of consent can be implicit (or tacit), particularly if these additional criteria are met:

a. If it does not involve sensitive information;

b. It does not violate the reasonable expectations of the individuals in the context;

c. If there is no risk of serious injury from the intended use or communication.

In this case, consent is not explicitly formulated. It is inferred by the organization from the silence or the inactivity of the individual concerned or from some other gesture of the individual that is not directly related to consent.

In practice, however, organizations should keep in mind that presumed consent (*Access Act*, s. 65.0.2; *Private Sector Act*, s. 8.3; see paragraph 14) covers many situations in which implicit consent might have been considered relevant. Cases where implicit consent to a secondary purpose is actually relevant are, however, less common.

[A priori non-compliant practice]

Example 36.1 – An elementary school offers an introductory activity to photography as an extracurricular activity for Grade 5 and 6 students. The parents validate the registration of their children by paying the related fees. In November, the registered students participate in a portrait workshop and take pictures of one another. The teacher in charge of the activity is particularly proud of the result. She selects five children's photos and sends them to the school administration to be published on the school's "parent portal", highlighting the activities offered by the school and the children's progress. Both felt that the parents agreed to this since they had been informed of the portrait workshop and since the "parent portal" is secure and accessible only to parents. **This implicit consent is probably not valid under these circumstances. Parents probably do not have a reasonable expectation that portraits of their child will be made available in digital format to several hundred parents without express consent. In the context of wide dissemination, photos of children could be considered sensitive, and the risks of serious injury from their dissemination would need to be properly assessed. For these reasons, the school should have relied on an express consent.** This could have been done by sending an electronic consent form to the parents concerned through the secure portal.

[A priori non-compliant practice]

Example 36.2 – An appliance leasing company receives an application to lease a refrigerator for a period of 48 months. The automatic acknowledgement of receipt sent to the customer indicates that the company will provide financing at a favourable rate for that period of time after a credit investigation by a personal information agent, whose name is listed in the email. In a separate section, the email states that if the customer does not respond, the company will provide the necessary identification information to the agent three days later. When the customer did not respond, the company proceeded with the credit investigation for financing, affecting his credit rating. The applicant then complained to the company that he intended to pay for the lease without obtaining financing. **In this situation, the company could not rely on implicit consent for the credit inquiry: It went against the reasonable expectations of the applicant, who had not requested financing, and caused him a significant prejudice by lowering his credit rating.**

[A priori non-compliant practice]

Example 36.3 – A city council agrees to deal with questions received by email from its citizens during its meetings. Citizens must identify themselves by their name and address. During council meetings, the questions are read aloud by the clerk, along with the names and addresses of those who submitted them. For transparency purposes, the meetings are recorded and posted on the municipal website for five years. No audio masking is done before posting, so names and addresses are publicly disclosed. When asked about this by a citizen, a council representative explained that he relies on implicit consent, believing that people who send questions by email should reasonably expect that their contact information will be released. However, no such information is provided on the city's website. **In these circumstances, the communication may not meet the reasonable expectations of the individuals and implicit consent may not be valid.**

[A priori non-compliant practice]

Example 36.4 – A start-up technology company wants to develop an artificial intelligence system to assess an individual's feelings based on his or her facial expression. In order to collect data to train its algorithm, it uses a data harvesting robot that scans various websites, including social networks and personal blogs, to extract photographs of faces. The company normally requires consent from third parties for this collection. However, the company believes that, by posting their photos on the web, individuals are implicitly consenting to their use for other purposes, including training an algorithm. **This collection could conflict with the reasonable expectations of individuals who share these photos with the idea that they will be seen by other individuals they know, but not that they will be used to train artificial intelligences.** Moreover, the individuals concerned cannot be informed of this practice in any way, causing a transparency problem.

37. Clear consent in all cases. When choosing implied consent, the organization must still be able to demonstrate that it was obtained in a clear manner. For example, the organization must be able to prove that the consent can be inferred (deduced) from another conduct of the individual. Such consent may be more difficult to demonstrate for the organization than express consent.

[A priori compliant practice]

Example 37.1 – A company that buys and sells auto parts wants to purchase an insurance (a policy covering theft and fraud committed by employees against the company). The company needs to obtain the credit report of each employee who will be covered by the insurance policy. It consults with the employees concerned to determine their comfort level with the policy. It explains that this involves checking their credit report by means of their name and address once, within five business days. The company asks them verbally whether or not they want to be covered by the insurance policy. This is the only question to which employees answer. **When employees accept coverage, they also implicitly consent to the communication of their name and address to their bank and to the collection of their credit report from the bank, since they have been properly informed.**

38. Other criteria. The other criteria for valid consent apply even if the consent is implicit. Thus, it must remain free, informed, specific, etc. In particular, the use of implicit consent is not a pretext for limiting the information given to the individual concerned regarding the planned operations with his or her personal information.

39. Cases of doubt. When there is doubt about the individual's true will regarding the use or communication of his or her information, the organization should obtain express consent.

2.2. Consent must be free

40. Free nature. Consent must be free, meaning that it must involve a genuine choice and control and be given without coercion or pressure. The individual concerned must therefore be able to exercise his or her will without being unduly influenced or suffering a disproportionate prejudice.

41. Fair mechanisms. It must be as easy to give consent as not to give consent. These options must be presented fairly. Consent mechanisms that do not ensure the fairness of the options or that influence the choice therefore lead to an invalid consent, since it is not truly free. For example:

a. Emphasizing acceptance over rejection renders consent ineffective, regardless of exactly how it is done (visual emphasis [colours, font size, etc.], efforts the user must make in number of clicks or web navigation, intentionally ambiguous wording, misleading text, etc.);

b. Repeatedly asking for consent when it has already been refused may violate its free nature. Consent can generally be sought only once for the same purpose, unless substantial change in the context justifies it.

[A priori compliant practice]

Example 41.1 – A municipality makes available an application to report various issues related to the maintenance of public spaces (snow removal, garbage collection, etc.). To create an account, users must provide an email address, which serves as an ID, and a postal code in order to initialize the area displayed by default in the maps available in the application. They can then access all services through the application itself and see the progress of their reports.

The application also allows them to use their email address to send them updates on the status of roadwork in their area. The agency provides a pop-up window to collect this consent. It has the "I accept" and "I decline" options at the exact same height, each placed in the same colour button with the same font size. **By ensuring the fair visual presentation of the choices, the agency ensures that the free nature of the consent obtained is not compromised.**

[A priori non-compliant practice]

Example 41.2 – A clothing store website allows customers to create an account to facilitate their online purchases. Each time a customer logs in, a pop-up window appears offering to send them the store's weekly newsletter with discounts that may be of interest to them. It is as easy to accept as to refuse this secondary use of the email address. However, if the customer refuses, the window will appear each time he or she subsequently logs in. **These repeated requests for consent, regardless of the customer's previously expressed will, may compromise its free nature. Practices of this type are not encouraged, as the validity of such consent could be challenged.**

42. Consent as a condition. To ensure that consent is freely given, an organization should generally avoid making it a condition of using a service, providing a good or obtaining employment. As a reminder, consent is presumed for the use and communication for the primary purpose if the individual provides his or her personal information after being duly informed (*Access Act*, s. 65.0.2; *Private Sector Act*, s. 8.3; see paragraph 14 above). Thus, when requested, it is generally for secondary purposes, which the individual should be able to refuse without affecting the original agreement.

If the operation subject to consent is necessary for the provision of the service or product, or for employment, the organization must make this explicit and explain the consequences of not doing so. The organization must also be able to demonstrate the reason why the operation is necessary in the circumstances.

[A priori compliant practice]

Example 42.1 – A public university explains in its application form for prospective students that the personal information collected will be used to assess the application, to create a permanent code and to communicate student status to the appropriate government department in the case of international students. It states that providing the information requested on the form constitutes presumed consent to these purposes, as per Section 65.0.2 of the *Access Act*. In a separate section entitled "Foundation", however, the university seeks consent for a secondary purpose: *"I consent to the release of my name, telephone number, email address, date of admission and field of study to the University Foundation for the purpose of philanthropic solicitation. This consent is valid for up to 5 years after my graduation.* ***Yes – No****".* **The university presents this secondary purpose, which is not essential to admission, in an appropriate manner. It gives the applicant the freedom to decline the communication, without affecting the rest of the application. In so doing, it ensures that the consent is free.**

[A priori non-compliant practice]

Example 42.2 – When selling a new car, a dealer uses a form to obtain the information necessary to grant the customer financing. In the consent section, it adds the following statement: *"By signing this contract, I agree that my email address and name can be used to send me promotional offers for the duration of the financing."* When questioned by a puzzled customer, the owner of the company indicates that this method is mandatory to receive financing. **This method does not allow refusal of the secondary purpose of sending promotional offers. The dealer therefore does not obtain valid consent since it is not free.**

43. Change of purpose. When an organization pursues a new purpose that is subject to consent (see paragraph 58), that consent may not be free if the organization indicates that it will cease to provide a service to those who refuse it. In such a case, the organization should again be able to demonstrate that the new purpose is necessary for the continuation of the service (see previous paragraph; see also paragraph 15).

44. Situations of imbalance. Situations in which there is an imbalance of power between an organization and an individual concerned may threaten the free nature of the consent. This is particularly the case in employer/employee relationships. The CAI recognizes that the law does not provide a ready-made solution in these circumstances. An organization must take steps appropriate to its context to mitigate this problem if it must rely on

consent. It may, for example, provide alternative ways of achieving the purpose so that an individual still has control over his or her information. In any case, it should pay particular attention to transparency so that the individual concerned is as informed as possible and that his or her other rights (complaint, access, rectification, etc.) are reserved.

[Practice whose compliance may vary according to the context]

Example 44.1 – During an intervention in a food company, the inspection team of an organization with oversight functions is photographed by its supervisor, who wishes to include the image in the intervention report. The company visited has been in the spotlight for a few months, and the media is interested in the inspection carried out by the organization. Following a media request, the supervisor sends an email to the employees who were present during the intervention to ask them if they agree to have the photo contained in the inspection report sent to a journalist to illustrate his article in the paper edition of the newspaper the next day. **Given the power relationship between the supervisor and the employees, care must be taken. If employees feel obliged to consent to this communication, the consent cannot be free. The supervisor must therefore be as neutral as possible in his request and not allow for any negative consequences if communication is refused.**

[A priori compliant practice]

Example 44.2 – A hospital decides to install a biometric access control system to restrict access to a room containing a machine functioning with highly radioactive material. Nuclear safety agencies' standards require particularly strong security to limit the risk of theft or sabotage of this type of material. Upon completion of the privacy impact assessment, the Access to Information and Privacy Committee approves the acquisition of a biometric system and declares the creation of a biometric characteristics bank to the CAI. In the consent form attached to the declaration, the hospital explains the purpose of the system and indicates that employees who do not want their biometric information collected will be able to authenticate themselves in other ways. They will need to present an access card and then validate their identity with a security guard. Both biometric and traditional access cards remain under the control of the individual. **In these circumstances, the hospital has made reasonable efforts to preserve the freedom of consent, despite the employment context: employees can refuse collection and opt for an alternative authentication solution.**

45. Link to granularity. Consent is free only if requested separately for each purpose (granularity; see Section 2.5). The options for the individual concerned should not be limited to accepting everything or refusing everything.

46. Withdrawal of consent. Free consent is also a consent that can be withdrawn at any time by the individual. Although consent is presumed in some cases (*Access Act*, s. 65.0.2; *Private Sector Act*, s. 8.3) and therefore has not been assessed as free, it may still be withdrawn as provided for in the statutes (*Access Act*, s. 65; *Private Sector Act*, s. 8). An organization must provide a simple and accessible mechanism for withdrawing consent and must notify the individuals concerned. The fact that an individual must make disproportionate efforts to exercise this right may have consequences on the free nature of the consent.

[A priori compliant practice]

Example 46.1 – A team from a university research laboratory is conducting a study on voice perception. The team recruits participants to record them reciting a text. Participants sign a consent form that includes all the required information and that allows the researchers to reuse their voices in further studies on the same subject for five years. Participants who, at some point, no longer wish to have their voices used by the laboratory can withdraw their consent by sending a simple email to the principal investigator. **This withdrawal mechanism is simple and accessible. It is not a barrier to obtaining free consent.**

[A priori non-compliant practice]

Example 46.2 – A music distribution company offers an application that allows users to access the albums they have purchased. A pop-up window appears when they first log in, allowing them to activate personalized recommendations to discover music. An algorithm then profiles them based on, among other things, the songs to which they listen, the length of time they listen to music and the time of the day during which they listen to music. Believing that these recommendations prevent him discovering music on his own by exploring the platform, a user decides to withdraw his consent to the use of this information for personalized recommendations. He has to make eight clicks in the different settings screens of the application before finding the option to disable the function. **While it takes only one click to consent to personalized recommendations, it takes many more to withdraw consent. In this context, the efforts are disproportionate and undermine the free nature of the consent on which the company relies.**

2.3. Consent must be informed

47. Informed. Consent must be informed, that is, specific and based on appropriate knowledge. The person concerned must know and understand what he or she is consenting to and what it entails. If the organization does not provide the necessary information, the individual's control is illusory, and the consent is invalid.

48. The individual's capacity. To be informed, consent must first be given by a person who is capable of binding himself or herself at the time of manifesting it (*Civil Code of Québec*, s. 1398). For example, consent given by a person who is incapable or under 14 years of age is not valid (*Access Act*, ss. 53.1 and 64.1; *Private Sector Act*, ss. 4.1 and 14). In these circumstances, however, it may be given by a representative, such as the person having parental authority or by the mandatary.

49. Information to be provided. In order to understand the reason that consent is being sought, the individual must be given access to the following information (in many cases, similar to the information that organizations must provide at the time of collection of personal information [*Access Act*, s. 65; *Private Sector Act*, s. 8]):

a. **Who?** The organization on whose behalf consent is being sought;

b. **Why?** Purpose for which consent is sought, i.e., the purpose for which the information is to be used or communicated;

c. **To whom?** If applicable, the names of the third parties or categories of third parties, outside the organization, to whom the organization will provide the information;

d. **From whom?** If applicable, the names of the third parties or categories of third parties, outside the organization, from whom the organization will collect the information;

e. **What?** Information, or at least categories of information, concerned;

f. **Accessible to whom?** Categories of individuals within the organization who will have access to the information in order to fulfil the purpose;

g. **Until when?** Length of time the consent is valid (see Section 2.7);

h. **And if not?** Consequences of not consenting or withdrawing consent at a later date (the organization must ensure that these do not compromise the free nature of the consent);

i. **With what risks?** Reasonably foreseeable risks or consequences associated with the operation covered by the consent, if any;

j. **How?** Means of using or communicating the information (e.g., postal communication; use of a fully automated decision);

k. **Where?** Place where the information will be communicated or stored in connection with the operation covered by the consent, including whether there is a possibility that the location may be outside Quebec;

l. **What rights?** Right to withdraw consent, right of access and right of rectification, with details on how to exercise them.

[A priori non-compliant practice]

Example 49.1 – A ministry employee asks an individual to sign a generic consent form **before completing all the fields**. The text presented to the individual reads as follows, with no information on the blank lines: *"I authorize the Ministry to release the following information: _____ to the following persons: _____ and for the following purposes: _____."* **This approach does not ensure informed consent.** The individual cannot understand the scope of what he or she is consenting to without having any information as to what is being consented to. When consent is sought, it must be given with full knowledge of the information involved.

[Practice whose compliance may vary according to the context]

Example 49.2 – Two online shopping platforms collect consent from shoppers to share their contact information with other companies, so that the latter can send them promotional offers. They use different texts:

- Platform A: *"I agree that [the Company] may share my contact information with partners."*
- Platform B: *"I authorize [the Company] to share my name and email address with its affiliated e-commerce businesses, so that they can send me promotional offers."*

Platform B's text is more comprehensive and more likely to lead to informed consent than Platform A's since Platform A does not disclose the purpose of the communication and does not provide any indication of the identity of its partners.

50. Accessibility of information – levels. Giving too much information at once to the individual concerned can be confusing. Nevertheless, all the information listed in the previous paragraph helps to ensure informed consent. To avoid overcomplicating the consent request, it may be advantageous for an organization to structure the information in several levels while taking into account the context of its activities. For example, information can be prioritized into two levels:

a. **First level**: Information that is immediately and effortlessly accessible, directly in the consent request.

    i. At a minimum, the **name** of the organization (who), the **purpose** (why) and the **third parties**, if any (to whom), should be mentioned at this level, along with the **information or categories of information concerned** (what), whenever possible. Elements that may be surprising to the individual should also be included (e.g., long period of validity, use of an unusual technology, numerous or significant risks, etc.);

b. **Second level**: Additional information that is easily accessible with minimal effort. In the oral modality, this second level could consist of a statement indicating that more information is available on request. In the written modality, this second level could consist of, among other things:

    i. A privacy policy accessible through a prominent link, especially when a technological means is used (*Access Act*, s. 63.4; *Private Sector Act*, s. 8.2);

    ii. An appendix to a form;

    iii. A question mark icon or a “Learn More” button next to the consent request.

[A priori compliant practice]

Example 50.1 – A school service centre (SSC) wants to fill a position that involves working with vulnerable people. It is then necessary to obtain a certificate of no criminal record from a police department. The SSC requires the consent of the candidates for this purpose. The hiring form contains a section dedicated to consenting to the release of information to the police department and to the police department’s communication to the SSC of the certificate of no criminal record created. **To ensure that this consent is informed, the SSC uses the following text, which reproduces the essential information from the consent request:**

“*SSC X* **[who?]** *needs your consent to communicate your identity information* **[what?]** *to Police Department Y* **[to whom?]** *to conduct a background search to certify that you can work with vulnerable individuals* **[why?]**. *This consent also covers the communication of the certificate of no criminal record* **[what?]** *to SCC X by Police Department Y. It is valid only until the certificate is actually provided* **[until when?]**. *If you refuse, we will not be able to proceed with your job application* **[and if not?]**. ***Additional information is available in Appendix A.***
☐ *I accept* / ☐ *I decline.*”

Appendix A provides the rest of the information, such as the right to withdraw consent, the right of access, and the right of rectification.

[A priori compliant practice]

Example 50.2 – An accounting firm uses some of its clients' personal information for secondary purposes with their consent, which it obtains through the electronic file available on its website. When consent is sought, the accounting firm states the purpose for which it is sought and the categories of information to which it relates. It specifies that the consent is valid for the duration of the next fiscal year. It also includes a link to a privacy policy. By clicking on this link, the user sees a pop-up window displaying a simple policy offering additional information (technical means of processing the information, location of storage, risks, explanation of the right to withdraw consent, the right of access and the right of rectification, and the contact information of the Privacy Officer). **By placing this information at a "second level", in an easily accessible privacy policy, the accounting firm ensures that an interested party can read it before consenting, while avoiding overcomplicating the consent request. The consent obtained is therefore informed.**

51. Precision and clarity of the terms used. The elements presented above should allow for a specific consent (see Section 2) through the use of simple and clear terms (see Section 2.5). An organization should therefore avoid vague, imprecise or overly complex terms, as well as long texts or texts full of legal jargon. These factors make it difficult for individuals to understand what they are consenting to.

52. Separate information for each purpose. When a consent request for secondary use or communication is made at the time of collection of the information, an organization must ensure that it provides:

a. All of the information required to meet its collection transparency obligations, including the primary purposes for which it collects the information (*Access Act*, ss. 65 and 65.0.1; *Private Sector Act*, ss. 8 and 8.1);

b. Information about the other purposes for which it seeks consent. However, it must do so separately (see Section 2.5, and Section 2.8 for written requests). Thus, there is a relationship between the informed nature of consent and the amount of information given at the same time to the individual concerned: presenting the information separately, especially if it concerns consent, reduces the potential for confusion.

[A priori compliant practice]

Example 52.1 – To address reports of harassment, incivility or sexual misconduct, a university collects personal information from complainants through a digital form. It provides an initial general text that explains the purpose of the collection, to whom the complaint must be communicated to ensure it is handled in accordance with the policy, and that the information is mandatory to process the complaint (with the exception of first and last name, which is requested on an optional basis). The rights of access and rectification are also presented. At the end of the form, once the complainant presses "Next," the university provides a separate page asking for consent to allow the office responsible for handling complaints to discuss the complaint with the management of the appropriate department. It provides the specific information related to that consent. **By providing the new information separately from the information regarding the collection of information necessary to process the complaint, the university promotes an informed consent to communication.**

53. Subsequent availability of information. Because a free consent can be withdrawn, the individual must have access to relevant information, even after consenting, so that he or she can re-assess his or her decision, if necessary. Thus, an organization should deploy means to make information easily available.

54. Duty to assist. An organization must provide assistance to individuals who require help in understanding the scope of the consent sought. It is responsible for developing mechanisms to do so.

[A priori compliant practice]

Example 54.1 – In order to have online access to the services of an organization that uses a third-party authentication service, an individual must consent to the communication of certain identity information by the third party to the organization. In its privacy policy, which is easily accessible through a link on the consent page, the organization notes that it is possible to chat with an agent to obtain assistance in understanding the consent requested. It also suggests speaking with an agent over the phone by providing a toll-free number that is accessible during business hours. **These mechanisms are part of the organization's tools for providing assistance to the individuals who need it.**

2.4. Consent must be specific

55. Specificity. Consent must be given for specific purposes, meaning that it must have a precise and circumscribed object. This criterion is strongly linked to the criterion of informed consent: an individual concerned can consent only if he or she is able to understand exactly what is being asked of him or her.

56. Specificity of the terms. An organization should be careful to use language that is as specific as possible about the purposes for which it is seeking consent. Vague, broad, or imprecise language threatens the specificity of the consent, and therefore its validity.

[A priori non-compliant practice]

Example 56.1 – A school seeks consent from parents for the multidisciplinary team to share information about the child's progress with a health care facility, where the child receives additional services. The parents are asked to consent that "*any information deemed necessary*" can be shared with "*any other person who needs it*". **The use of such imprecise language compromises the informed nature of parental consent, as well as its specificity.** The school should precise the specific purpose(s) intended, which in this case is to allow for better support of the child by the health care facility as part of the additional services. The school should also provide details about the information concerned and the anticipated frequency of communication, as well as specify the intended categories of recipients (e.g., "*professionals assigned to the child's care at health facility X*").

[A priori non-compliant practice]

Example 56.2 – A union seeks explicit consent from some of its members to use some of the personal information contained in active complaints to "*improve its processes*". **This term is imprecise and undermines the specificity of the consent, as it does not provide a clear understanding of the purpose.** The purpose should be more clearly stated (e.g., "*training staff*", "*training artificial intelligence to automate certain steps in the complaint process*", etc.).

57. Restriction on use. In order to respect the specific will of the individuals concerned, an organization must rely on consent only for what it allows. Expressed consent is restrictive: it is valid only for the specified purposes or third parties. Misuse, which occurs when the organization makes an unintended use or communication of information that is not in accordance with the consent of the individual or the purposes identified at the time of collection (unless the legislation provides an exception, such as consistent purposes), is a privacy risk and a confidentiality incident (see paragraph 16).

[A priori non-compliant practice]

Example 57.1 – An intermunicipal board is asked by a company to provide the final year's attendance record of one of its employees who is seeking a position within the company. The intermunicipal board's human resources director (HRD) contacts the employee in question to obtain her consent to provide the record to the future employer, which the employee accepts. However, the HRD sends the employee's complete attendance record, which covered four years of service. **In doing so, the HRD did not respect the specific consent that had been obtained, which related exclusively to the disclosure of the last year's attendance record.**

[A priori non-compliant practice]

Example 57.2 – An individual who purchases a television and a computer online consents to the retailer's providing his contact information and purchase information to three partner companies, specifically named in the consent request, in order to receive promotional offers from them. Two months later, the retailer establishes a business relationship with two new partners and shares the information with them as well. **However, the retailer cannot do so under the original consent, as it was specifically directed to the previous partners.**

58. New purpose, new consent. Where an organization wishes to use or communicate personal information for a different purpose than the one to which individuals have already consented, it must obtain a new consent, unless a legal exception applies (see paragraphs 9-13).

2.5. Consent must be granular: it is sought for each purpose

59. Granularity. Consent must be granular, i.e., requested for each purpose. Granularity refers to the image of a material whose parts can be distinguished.

60. Well-defined purpose. To meet this criterion, an organization must define as much as possible the scope of the consent, in proportion to the purpose. In other words, if there are multiple purposes, it should provide for specific consent for each purpose separately. Granularity ensures that consent is truly free. It is not free if the individual must accept several purposes at the same time. In this case, the only option is to refuse or accept as a whole, which does not represent all the nuances of the individual's will. Similarly, granularity ensures that the person expresses his or her will clearly for each specific purpose.

[A priori non-compliant practice]

Example 60.1 – An organization funding projects collects applications through a form. It wishes to seek consent for two purposes: (a) communication of the applicant's contact information to a broadcaster for the purpose of promoting the selected projects, and (b) use the email address for the purpose of sending a survey. It provides a "consent" section, where these two requests are made successively, and then adds a single "*I agree*" box and a single "*I decline*" box. **By doing so, the organization compromises the granularity of consent by asking one authorization for two purposes.** It should be possible for individuals to consent to the communication of their contact information for promotional purposes, but not consent to the use of their email address for survey purposes, or vice versa.

[A priori compliant practice]

Example 60.2 – A non-profit organization organizes a gala event to present awards to practitioners in its field. The organization collects the email addresses of nominees to inform them of their nomination and the details of the ceremony. The organization also asks the nominees to consent to three secondary purposes: (a) to use their email address to contact them to assess their satisfaction after the event; (b) to use their email address to send them the organization's general newsletter; and (c) to allow the company designated by the organization to take the official photos of the award winners to retain their email address in order to offer them discounts on other photography services. **In order to respect the granularity of consent, the organization arranges these three purposes in a table with a "Yes" column and a "No" column to allow nominees to accept or decline each of these three purposes separately:**

"*Consent. Do you consent to your email address being:*

- *Used to contact you to assess your satisfaction after the event?*

☐ *Yes* ☐ *No*

- Used to send you our general newsletter?

☐ *Yes* ☐ *No*

- Kept by the company designated to take official photos of the award winners to offer you discounts on other services?

☐ *Yes* ☐ *No*"

2.6. The consent request must be understandable: it must be presented in simple and clear terms

61. Understandability. The consent request must be understandable, i.e., presented in simple and clear terms, both in terms of the information and of the specific statement of acceptance or refusal. This criterion is intended to ensure not only that the consent is informed but also to prevent the organization from interpreting the consent too broadly at a later date (specificity of consent). There are various elements that can simplify and clarify statements for individuals concerned, including those discussed in the following paragraphs.[4]

[4] The plain-language web writing principles of the Quebec.ca government design system can be a useful resource: https://design.quebec.ca/contenu/principes-redaction/langage-clair-simple [*in French only*].

62. Conciseness. Statements should be concise, i.e., expressed in as few words as possible, while remaining clear. An organization should avoid superfluous words, complex structures and too much circumlocution. Overly long sentences or texts are detrimental to the understanding of the individuals concerned.

[A priori compliant practice]
Example 62.1 – In a consent form for financial assistance, a ministry uses the following wording: "*I authorize the Ministry **to forward as soon as possible to the rehabilitation service provider all information related to holding an account with a financial institution in order to proceed with the payment of my financial assistance, if applicable**.*"

When completely revising its form, the ministry changes it for the following: "*I authorize the Ministry **to forward to the rehabilitation centre the details of my bank account in order to pay my financial assistance**.*"

This improves the conciseness and the clarity of the statement without losing crucial information.

63. Simplicity of vocabulary. An organization should use simple language, i.e., language that is accessible to the individuals concerned. It should use common vocabulary, without legal or organizational jargon.

[A priori non-compliant practice]
Example 63.1 – A grocery store offers a loyalty application to its customers, who receive points redeemable for discounts for each purchase. They can view their purchase history for the past year in the application. The grocery store decides to deploy a system of personalized discounts according to buyer profiles, which it wants to determine from their transactional history. To do so, it solicits the consent of the application's users with the following text:

"***Receive personalized offers*** *– By checking "Yes", the Customer agrees to the automated analysis by the Company, including, but not limited to, historical transactional data for the purpose of determining a profile by machine learning model; said profile will be used by the Company to issue, without however formally committing to it and subject to its policies and procedures in force, personalized offers of discounts on the purchase price of certain products, provided that the Customer complies with the Terms of Use.*"

This legal style text contains several words that are not common vocabulary and several complex turns of phrase (long sentence, etc.). It can confuse the individual concerned, thus compromising his or her informed consent. The following text would be simpler, and therefore more understandable:

"***Receive personalized offers*** *– By checking "Yes", I authorize the company to use my purchase history to determine my buyer profile using an artificial intelligence system. The company will be able to choose to send me personalized discount offers tailored to my profile if I follow the terms of use of the loyalty application.* ☐ *Yes* ☐ *No*"

64. Clarity of intentions. An organization should use the most direct terms possible to ask the individuals for permission, both in the way it is presented and in the wording of the options available to the individuals. The use of specific language avoids all confusion about what the individual has to do and preserves its legal meaning. Similarly, language expressing uncertainty or assumption (e.g., conditional verbs) should be avoided unless the organization can demonstrate why such use is unavoidable.

[A priori compliant practice]

Example 64.1 – An organization reviews its procedures for obtaining consent according to a schedule set out in its governance rules. The committee formed for the occasion notes that the consent requests are generally introduced by vocabulary referring to knowledge rather than permission: "I am *aware* that information X will be used [...]" or "I *understand* that information Y will be communicated to [...]".

In order to clarify these requests, the committee modifies them so that the verbs clearly evoke consent: "I *consent* to [...]," "I *agree* that [...]" or "I *authorize* the use of [...]."

The committee also notes that the explicit consent options on web interfaces do not reflect the consent situation (acceptance or refusal). In many cases, the options provided are "*Next*" or "*Ignore*," while in other cases the wording of the options emphasizes acceptance versus refusal. For example, a consent pop-up window offers users the option of pressing "*Yes!*" or "*Maybe later*." **On the recommendation of its committee, the organization homogenizes the options to present a choice between "Yes" and "No" as often as possible**, or, alternatively, "*I agree/I consent*" and "*I decline/I do not consent/I disagree*."

With these changes, the organization is moving towards clearer and simpler language, and it is promoting informed and free consent.

65. Adaptation to the audience. Information should be adapted to the targeted audience. An organization needs to consider the perspective and profile of the individuals to whom the information is directed: the individuals may not always be familiar with their privacy rights, nor with the organization's activities, and some may not be fluent in either spoken or written language. The organization should also adapt the language used to the lowest level of literacy among the various categories of individuals concerned to whom a request for consent is addressed.

[A priori compliant practice]

Example 65.1 – At the request of an Indigenous Nation that is intensifying its language revitalization efforts, a team of researchers conducts an in-depth language study with elders from the Nation in partnership with an Indigenous cultural institute. In order to analyze the data, the words of these elders are recorded in different situations (outing on the territory, family discussion, craft session, etc.). The participants are notably asked to tell a traditional story. The cultural institute would like to ask participants to consent to having the recordings of these stories posted on a section of its website dedicated to the Nation's language and to the preservation of its intangible cultural heritage. To do so, it uses a French form. However, some of the older participants speak very little French. **In order to ensure that the consent form is adapted and that it is understandable to them, the cultural institute mandates a bilingual agent to collect the oral consent of these participants and to answer their questions, if necessary.**

[A priori compliant practice]

Example 65.2 – A company offers a photo-sharing application to a diverse population, including 14- to 17-year-olds. In order to ensure that its consent procedures are clear to them, the company conducts comprehension tests with about a hundred of users and makes the required changes. By adapting the texts to the literacy level of adolescents, it increases the likelihood that the texts will be understandable to most of its clienteles. In this way, the company ensures that the terms are simple and clear for the individuals concerned.

2.7. Consent must be temporary: it is valid only for the time necessary

66. Temporary nature. Consent must be temporary, meaning that it must be valid for a limited period of time. It is valid only for the time necessary for the purposes for which it was requested. Thus, it is no longer valid once these purposes have been fulfilled.

67. Limitation of duration. The time limitation may be related to two types of conditions:

a. **A time limit:** The purpose may be considered fulfilled after a period of 30 days, one year, six years, etc. The time limit may also be set by statute, such as the *Archives Act* (CQLR, c A-21.1).[5]

b. **An event:** The purpose may be considered fulfilled when an event occurs – as soon as a payment is completed, as soon as a student leaves the university, as soon as a contract ends, etc.

[A priori compliant practice]

Example 67.1 – As part of its hiring process for professionals, an organization asks candidates to provide two references that can be used to assess their performance in previous positions, in addition to the evaluation information in their files. It provides an electronic form for submitting references. **In order to make the consent temporary, the organization specifies that it is valid only until a decision is made regarding the application. This consent is therefore delimited by an event.**

68. Link to specific and informed consent. In order to be able to provide specific and informed consent, individuals concerned must be informed of the duration of the validity of their consent. Again, vague or imprecise language should be avoided. If the end of consent is related to an event, an organization should provide sufficient information to the individual concerned to enable him or her to know how long consent is likely to last or to estimate when it will end. The organization should also inform the individual of his or her right to withdraw consent at any time (see paragraph 49).

[5] The CAI is not responsible for enforcing this statute.

69. Transparency in relation to long-term consents. When an organization seeks consent for a very long period of time, it should pay particular attention to transparency on an ongoing basis. It could remind the individuals concerned, at appropriate intervals, that it is using or communicating their information on the basis of consent, referring them to updated information on this situation (see paragraph 53) and reminding them that they may withdraw their consent at any time. The organization could also disseminate this information through an easily accessible medium (e.g., a website), which may be useful, for example, when it is not possible to reach the individuals concerned.

2.8. The consent request must be separate: it is submitted separately if it is made in writing

70. Distinctiveness. If the consent request is in writing, it must be presented separately from any other information. It is therefore separate from terms of use, broader privacy policies, requests for confirming the validity of the information provided, undertakings, signatures, etc. It must be featured in its own section or interface (form section, pop-up window in an application, etc.), so it is easily accessible to the individual concerned.

71. Link to other validity criteria. The distinctiveness of the consent request is interrelated with other criteria for the validity of consent, including the following:

a. **Clear and free**: Consent is not clear if it is expressed by a gesture that may also indicate something else, such as the receipt of an information or the validity of the information provided, since the intentions behind the gesture are then inseparable (see paragraphs 35 and 42). Nor is it free since it is difficult to express a refusal in these circumstances;

b. **Informed**: Separate consent requests help to limit the amount of information provided at the same time and thus facilitate the understanding of the person concerned.

[A priori non-compliant practice]

Example 71.1 – At the end of a change of status form of a professional order, the individuals concerned must sign after four statements:

"*1. I acknowledge that I have read the notice […].*
2. I declare that the information provided is complete and accurate [...].
3. I agree that the Order may communicates my information to the insurer [...].
4. I agree to notify the Order of [...]."

The request for consent (third statement) is not presented separately from any other information, as it appears among three other statements that are not consents. This also undermines the clear and free nature of the consent. To correct this situation, the Order could move the consent request to the beginning of the section, add "*Yes*" / "*No*" boxes and indicate that the signature is valid only for the other three statements:

"***Consent.*** *I consent to the Order's sharing my information with the group insurer [...].*
☐ *Yes* ☐ *No*
By signing this form:

✓ *I acknowledge that I have read the notice [...].*
✓ *I declare that the information provided is complete and accurate [...].*
✓ *I agree to notify the Order of [...].*"

[A priori non-compliant practice]

Example 71.2 – When completing the creation of an account for an online game, players are asked to check a box stating that they agree to the terms of use, to which a hyperlink is provided. However, no reference to consent is included in the form. By clicking on the link, players may discover that the terms of use contain, among other things, the publisher's privacy policy. It is stated in the text that, by accepting the terms of use, the players consent to the use of their friends lists, device metadata, interactions during the game (clicks, hours, etc.) and conversations on the public server for purposes of targeted advertising, improving the game experience and fighting cheating, among others. They also consent to the dissemination of their in-game scores on a public platform, along with their nicknames and game histories, in order to stimulate competition in the game.

On the specific issue of consent, the fact that this information is embedded in a privacy policy that is itself embedded in terms of use that address a variety of other topics undermines the distinctiveness of consent. Moreover, this situation threatens its clear nature (gesture of consent inseparable from the gesture of acceptance of the terms of use), its free nature (granular refusal impossible) and its informed nature (information difficult to access).