Commission d'accès à l'information du Québec

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 Privacy Act (see updated administrative versions on its website). It has the function of developing guidelines to facilitate their application. With the upcoming coming into force of the bulk of Bill 25, which amends these Acts, 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, found on page 4 of this document (**go directly to** them), are intended to assist organizations and individuals subject to these Acts to better understand the relevant elements in assessing each statutory criterion for valid consent (Act respecting access to documents held by public bodies the the protection of personnal information, section 53.1; Privacy Act, section 14). The guidelines are illustrated with examples. **The guidelines do not apply to the health sector[1] .**

Consultation

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, it 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 laws:** a questionnaire is available on the Consultation Québec platform. It allows to comment briefly on the proposed text and to formulate suggestions for future guidelines.
2. **Stakeholders previously identified**: 18 stakeholders identified by CAI for their expertise, representation or 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.

Partly in keeping with its organizational capacity to analyze comments, CAI is conducting a mixed consultation, part of which is by invitation. 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 provides a framework for health information, are not included in the scope of the guidelines, as it will be a separate framework.

Analysis of comments and feedback

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

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

Influence of the approach

The comments received will allow the text to be adjusted, if necessary. Examples, the level of detail in the text, and the format of the text will all be subject to change. CAI's general approach to the sections of the Act, on the other hand, is less likely to change and will only be modified if the comments reveal something new in the analysis.

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

Limits of the consultation

CAI:

- **Will not provide individualized responses to** questions about legislation submitted during this consultation;
- **Will not process any submissions without an 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.
    - 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 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.

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, ext. 51113.

List of stakeholders who will file a brief

1. Secretariat for the Reform of Democratic Institutions, Access to Information and Secularism
2. Ministry of Health and Social Services
3. Quebec Bar
4. Fédération des centers de services scolaires du Québec
5. Quebec Research Fund
6. Association of Information Access and Privacy Professionals (AAPI)
7. Fasken Martineau DuMoulin, LLP
8. Border Ladner Gervais, LLP
9. Gowling WLG (Canada), L.L.P.
10. Lavery de Billy, L.L.P.
11. Federation of Quebec Chambers of Commerce
12. Conseil du patronat du Québec
13. Canadian Life and Health Insurance Association
14. Canadian Bankers Association
15. Canadian Marketing Association
16. International Observatory on the societal impacts of AI and digital technology
17. Consumer option
18. League of Rights and Freedoms

Commission d'accès à l'information du Québec

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 effect on September 22, 2023)

Version 0.1 - Document for consultation

(note: these guidelines are not yet in effect)

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 pursuant to section 123 of the *Act respecting access to documents held by public bodies and the protection of personal information* (hereinafter the ATIA).

2. **Purpose.** CAI is issuing these guidelines to facilitate understanding of the criteria for valid consent that public and private organizations (hereafter[2]) must obtain from an individual to whom personal information relates. These criteria include:

    a. In the ATIA, in section 53.1;

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

    In this document, unless other sections are explicitly mentioned, the guidance is intended to interpret 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 (ATIA, sections 23, 24, 25 and 49).

    Nor is it intended to provide specific guidance on when consent is or is not required, except for the general information provided in section 1.1. It focuses on the criteria to be met when consent is indeed required by law.

4. **Legal References.** These guidelines are based on the ATIA and PA as amended by the *Modernization of Personal Information Protection Legislation Act* (S.Q. 2021, c. 25, or Bill 25). The CAI makes available administrative versions of the ATIA and PA incorporating the Bill 25 amendments.

5. **Examples.** The examples given in these guidelines are fictitious, but may be based on actual practice. They are simplified to highlight specific consent issues and thus illustrate a particular 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. Sometimes a single example will accompany a paragraph, when CAI considers that it illustrates its meaning well 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* (R.R.S.Q., c. S-4.2), or general legislation, such as the *Civil Code of Quebec* (R.R.S.Q., 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" covers even individual companies in the context of these guidelines.

1.1. Consent is at the heart of the principle of control by of their personal information

7. **Notion of consent.** By default, personal information is confidential. Individuals can exercise control over the use and flow of their information through consent. Linked to personal autonomy, consent implies that they agree to what happens to their information. Consent is an important concept in Quebec's privacy legislation.
To comply 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 a minor under the age of 14 (ATIA, s. 64.1; PA, s. 4.1) - consent is given by the parent or guardian;

b. To collect, in the private sector, personal information from a third party (PA, section 6);

c. To use personal information for a secondary purpose, i.e., a purpose other than that for which it was collected (referred to as the primary purpose) (ATIA, s. 65.1; PA, s. 12);

d. To communicate or disclose personal information to a third party (ATIA, sections 53, 59 and 88; PA, sections 13 and 40).

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

9. **Exceptions.** In some cases, the ATIA and PA provide exceptions that allow an organization to use or disclose 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 (ATIA, s. 52.2; PA, s. 3.1; see section 1.3), an organization must be able to demonstrate that an exemption allows it to use or disclose 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 document. In this way, individuals are informed of what happens to their information each time the organization collects, uses or discloses it, thus preserving their rights: access, rectification, de-indexing, complaint to the organization or 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, especially where there are no practical difficulties in obtaining it (e.g., small number of individuals involved, easy to reach, non-emergency situation, etc.).

Depending on the context, consent may sometimes be more advantageous to the organization, for example to facilitate demonstrable compliance with the law (see section 1.3). Importantly, consent can also be withdrawn at a later date by the individual (see Section 2.2), adding a means of control over 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 an organization chooses to rely on consent rather than an applicable exception for the collection, use or disclosure of personal information for a specific purpose, it must respect the choice of the individual. Thus, it cannot, for that same purpose, go back and choose to rely on that exception if those individuals refuse to consent or withdraw their consent. To do otherwise would render consent meaningless as a means of controlling individuals.

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

14. **Deemed consent**. When an individual provides his or her personal information after having received the statutory information (ATIA, section 65; PA, section 8), he or she is presumed to consent to its use and disclosure for the purposes for which it was collected and of which he or she is informed (ATIA, section 65.0.2; PA, section 8.3).

This presumed consent means that the organization is not required to assess its validity criteria. However, the individual can withdraw consent at a later date.

15. **Consent and necessity. At** all stages of the life cycle of personal information, i.e., collection, use, disclosure, retention and disposal, the law places a limit on the necessity of the information to accomplish the purpose (e.g., ATIA, ss. 64, 65.1, 67; PA, ss. 5, 12, 18).

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

[A priori non-compliant practice].

Example 15.1 - At its general meeting, a sixteen-member association
A co-owner adopts a unanimous resolution for the installation of surveillance cameras capturing images in all the corridors of a condo building in order to ensure the security of the premises. However, there is no history of problems with
security. The purchased cameras are placed in an angle that allows

film the front door of each unit.

Despite the unanimous agreement of the co-owners, which indicates their consent, capturing images throughout the building is likely to be, with respect to

the impact of the cameras on the privacy of the co-owners and their guests is not proportional to the security objective pursued. Indeed, people have an expectation of privacy when they are in residential premises; however, the angle of the cameras means that they record and document their comings and goings, people that they frequent, etc. In addition, the safety issue is theoretical and not proven, since no previous incidents have occurred. In these circumstances, the condominium association's collection of videotapes does not meet the necessity, and consent is not sufficient to bring it into conformity with the law.

16. Privacy incident. Accessing, using or disclosing personal information without the consent of the individual, when the law requires it, is a privacy incident (ATIA, s. 63.9; PA, 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 ATI and the individuals concerned if there is a risk of serious harm, 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. When organizing a holiday event, two employees in the department use these banking details to send an electronic funds transfer request to those who have confirmed their participation in the event and who must pay for their registration. This secondary use is not authorized by any statutory exception and the employees did not consent to it. This is a privacy incident for the municipality. The municipality must record it in its registry and assess the risk of serious harm to the individuals involved to determine whether to notify them and the CAI.

[A priori non-compliant practice].

Example 16.2 - A social network offers users the option 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 to serve ads to users who are already in their own customer lists. To do this, the publishers upload their list, in encrypted format, to the social network tool, and the algorithm checks whether the customers are users thanks to different information. Among other things, it takes into account the phone number and email address contained in the users' profile, which it compares to marketing lists. In doing so, the social network uses this personal information without This is a privacy incident, as the consent of the individual was not obtained and no exceptions (compatible purposes, security reasons, law enforcement, clear benefit to the individual, etc.) apply. This is a privacy incident.

1.2 These guidelines represent the Commission's expectations

17. Who is affected. These guidelines are specifically intended for the following individuals within an organization:

a. The person with the highest authority;

b. The person responsible for the protection of personal information;

c. Members of the Public Sector Access and Privacy Committee;

d. Staff who work in privacy, service design or information technology;

e. Staff who collect consents related to personal information.

18. CAI's intent. These guidelines represent CAI's expectations of organizations with respect to obtaining valid and meaningful consent. The additional clarification they provide is intended to facilitate enforcement.

19. Strength of guidelines. Guidelines are more important than CAI 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 implement them. If they do not, they should be able to explain why.

21. Evolution. These guidelines may be modified at a later date and others, more targeted to certain sectors of activity, for example, could complement them.

1.3. Organizations must be able to demonstrate compliance

22. Accountability principle. Organizations are responsible for protecting the personal information they hold (ATIA, section 52.2; PA, section 3.1). They must be able to demonstrate that they are complying with their statutory obligations (demonstrability principle), 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 must develop methods that are appropriate to their 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 the obtaining of consent for the release of certain tax information to a third party, a department decides to retain audio recordings of entire telephone conversations during which
the persons concerned give their consent to an agent. This method is

likely to fail the minimization principle, as it results in the collection of additional information (audio recording, full conversation) only to demonstrate compliance. Instead, the department could note
the date and time of the consent, as well as the name of the member of the staff who collected it.

[A priori non-compliant practice].

Example 23.2 - An insurance company wishes to document its obligation to obtain consent for the disclosure of
compensation information to a third party. Through its web form, it
decides to record the users' cursor movement pattern on the consent page, from its opening until they check the "I consent" in order to prove that the gesture is reflected She also records the duration of the transaction. This method may not meet the princi ple of minimization, since it involves the collection of additional information
The insurance company could instead record only the checked status of the box, as well as the date and time the box was checked. 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' folder.

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

[A priori compliant practice]

Example 24.1 - A Crown corporation offering digital services keeps an archive with screenshots of its online consent form.
Each one is accompanied by an indication of the time period it represents. Each time change is made to the form, the Crown corporation adds a new screenshot to its archive. This practice allows the Crown corporation to keep a record of the elements used to assess the validity of a consent obtained at a particular time.
in the past, especially in the context of an inspection.

[A priori compliant practice]

Example 24.2 - A company operating a call center has a policy and procedures related to customer consent to disclosure of personal information. One of the procedures, which sets out a framework for service requests, has been updated three times in recent years.
In each case, the company kept a copy of the previous versions. In case of
the need, it ensures that it can more easily demonstrate that a consent
obtained when applying a previous version of the procedure was indeed illuminated, for example.

25. Authentication of the data subject. Since consent is an expression of personal will, an organization must ensure that it obtains consent from the individual (or his or her legal representative, if applicable). In order to do this

In doing so, the organization should aim for a reasonable degree of certainty, depending on the context of its activities. Where there is a legal representative, the organization should also verify the status of the person giving consent (parental authority, legatee, representative, etc.), always with a reasonable degree of certainty. This verification can be accomplished by validating certain personal information, but the organization shall 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 it.

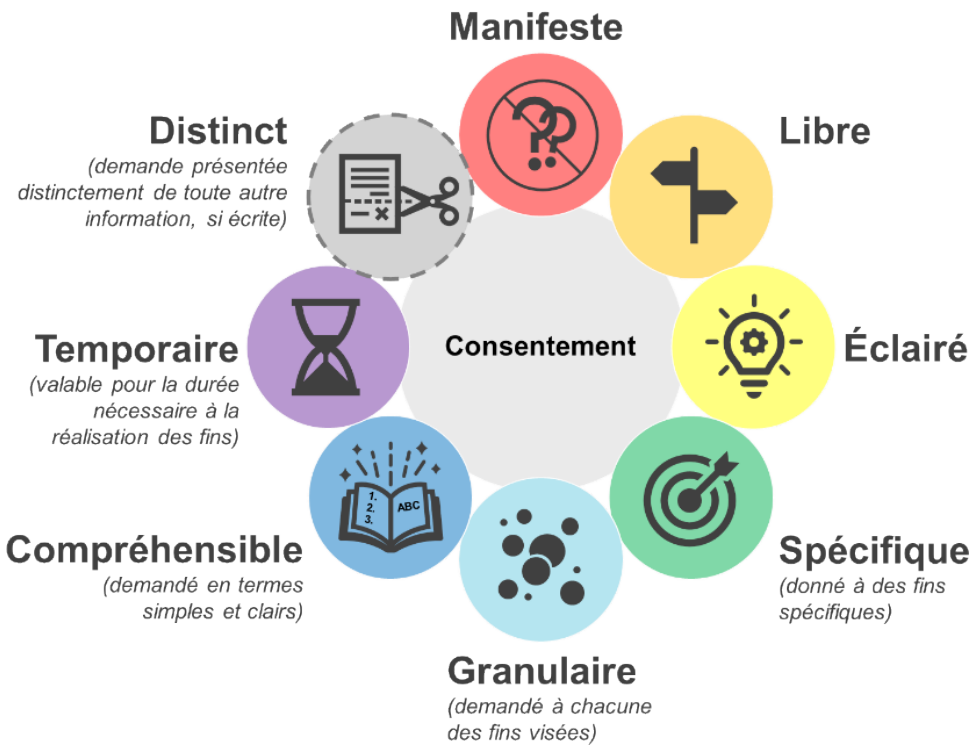
2. CRITERIA FOR VALID CONSENT

27. Criteria. Valid consent is defined in sections 53.1 of the ATIA and 14 of the PA, which contain eight criteria (each text box is a link to a specific section of these guidelines):

"A consent [provided for in the law] must be manifest, free, illumin and given for specific purposes . It is requested for each of these ends in terms simple and clear. When the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned . When the latter requires it, it is assisted in order to understand the scope of the consent .

[...]

Consent is only valid for the time necessary to achieve the purposes to whom it has been requested.
A consent that is not given in accordance with [the law] is of no effect."



28. **Interrelationship between criteria and importance of each.** The criteria are interrelated. They are all important: if one of them 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 links between the criteria are clarified.

2.1. **Consent must be evident**

29. **Manifest.** A consent must first be manifest, 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 takes an active step (or makes a statement) that clearly indicates 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 seek express consent whenever possible.

31. Mandatory Express Consent. In some situations, the organization must obtain express consent. For example:

a. **Sensitive information:** The use or disclosure of sensitive information must be authorized by express consent (ATIA, sections 59 and 65.1; PA, sections 12 and 13).

i. Sensitive information is information that is medical, biometric,[3] or otherwise intimate in nature, or the context of its use or disclosure gives rise to a high reasonable expectation of privacy (ATIA, section 59; PA, section 12);

ii. Consent is not required for the use or disclosure of sensitive information for the primary purpose for which it was collected (ATIA, s. 65.0.2; PA, s. 8.3) or where exceptions to consent apply.

b. **Identification, tracking and profiling:** Legislation requires that technologies that identify, track or profile individuals be turned off by default; organizations must inform individuals of the means to turn them on (ATIA, s. 65.0.1; PA, 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. When collecting information to pay the allowance,
the agency made no mention of using it for evaluation purposes. In order for the evaluator to use the information of the 275
In order to ensure that the consent of the recipient is unambiguous, the agency develops a self-supporting form and sends it to the recipient so that he or she can provide it to the agency. To ensure that this consent is unambiguous, the agency develops a self-supporting form and sends it to recipients to sign it.

[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 partners
based on their proximity. In order to access this feature, users must enable 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 provides them with
then explicitly asks for permission to activate the geolocation.

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

[A priori non-compliant practice].

Example 31.3 - A Crown corporation must produce statistics on the diversity (gender, ethnic, linguistic, etc.) of its workforce in order to create a action plan against discrimination. Not having access to information on sexual orientation of employees, the human resources team will consider using the gender information of their dependent spouse from the group insurance plan for each employee, in order to calculate the proportion of staff with a same-sex spouse. In these circumstances, the company must ensure that it obtains the express consent of employees, since the gender of their spouse is a sensitive information: it is very likely to reveal sexual orientation, a information protected by the *Quebec Charter of Rights and Freedoms*.

[A priori non-compliant practice].

Example 31.4 - A massage therapy clinic hosts a series of health and wellness conferences in conjunction with other health care providers. The owner wants to send personalized invitations to her clients. She plans to use their health and medic al history, collected during the opening of their file to ensure that the treatments offer ed are safe, to invite them to attend conferences relevant to their situation. This secondary use of sensitive (medical) information cannot be carried out without express consent. Having not requested such consent in advance, the clinic owner finally decided to advertise the conferences in the clinic's newsletter already sent to clients who had agreed to receive news about events.

[A priori compliant practice]

Example 31.5 - After a series of attempted break-ins, a company manufacturing explosives wants to strengthen access control to its storage site in to limit it to authorized personnel only. The company is considering the purchase of a biometric handprint recognition system. After conducting a privacy impact assessment that takes into account the context of its operations, the company concludes that its situation justifies the use of this technology. Since the system relies on biometric characteristics, the company recognizes that it needs express consent and develops a consent form for the collection and use of these characteristics for the purpose of authenticating authorized personnel.
Employees who wish to do so can sign it and those who refuse can opt for an electronic access card system.

32. Method of obtaining. An organization is free to develop express consent mechanisms that are appropriate to its business, as long as they comply with the law. These mechanisms should be tailored to the individuals involved, 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, 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 motor difficulties, the majority of whom cannot write or use touch screens. In order to validate financial assistance, they must provide

information on their file to a department.
For example, the rules of governance of the organizations exclude the use of exceptions to consent where it is practically easy to obtain (e.g., where a small number of individuals are involved). The employee must therefore rely on the consent of the individuals concerned for the disclosure of the information. The employee will ask for consent orally and record the date, time and details of the consent in the file notes to meet the demonstrability requirement. This mechanism allows for demonstrable consent (in this case, explicit consent) 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 ages 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.
During its configuration, the toy gives auditory instructions to the parents. For consent to the collection of the child's progress information, they will requires the simultaneous pressing of three colored buttons located on the front of the toy. This mechanism allows to obtain a manifest consent (explicit, in this case) case) taking into account the device with which the parents interact.

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 actions can make them meaningless, it is important that the person concerned is 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. Due to the nature of its business, citizens frequently interact with this application. Thus, the organization often collects consents. It asks users to confirm them by answering a mathematical question (such as 8 + 4). In this way, it helps to "break the rhythm" and partly combats consent fatigue.

[A priori compliant practice]

Example 33.2 - A bank's application frequently asks its customers for consent to disclose their personal information. When it needs to, it displays, on a random basis, a window overlaying the application showing 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 of them. The accept or decline consent buttons do not activate until the time limit has passed. By doing this, the bank is "breaking the rhythm" and partly combating consent fatigue.

34. Inadequate methods. Even allowing for consent fatigue, an organization cannot *assume* express consent: it must involve an active and positive (unequivocal) gesture. The following methods of obtaining consent are therefore not valid, since they do not ensure beyond doubt the will of the person concerned:

a. Use of already checked boxes;

b. Simple possibility to refuse later (*opt out*);

c. Deduction related to the silence or inactivity of the person;

d. Deduction related to another action taken by the person.

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 efficiently to citizen requests, an organization wants to develop an artificial intelligence system (AIS) to prioritize cases. It plans to develop the AIS based on data on the use of its services over the past three years. Its Access to Information and Privacy Committee, upon completion of the assessment The Privacy Impact Assessment found that express consent was required to use the information for this new purpose. Despite this, the organization decided to send an email to the individuals concerned informing them of this new use, and stating that they could contact the organization's Privacy Officer to withdraw their consent to this use. Since the organization assumes consent and does not offer individuals the opportunity to affirmatively opt-in, it does not obtain express consent. This could have been done, 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 - Magazine Web site offers recommendations
personalized articles 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 profiling, the magazine displays a window overlaid on the content during the first visit to the site and provides the persons concerned with the information required by the LP (articles 8 and 8.1, in particular). They then have the option of
the ability to accept or decline cookies for personalization purposes
recommendations. To do this, two clearly identified buttons ("*Accept*" /
The "*Refuse" button*, highlighted in the same way, appears at the bottom of the overlay window. This allows the magazine to obtain consent

35. Risk of confusing the individual's intentions. For consent to be express, an organization must avoid confusion with another action taken by the individual, such as confirming that the terms and conditions have been read

of use. It must design clear consent mechanisms for data subjects. This is related to the distinctiveness of consent (see section 2.8).

2.1.2. *In some situations, consent may be implied*

36. Possibility of implied consent. In certain circumstances, the form of consent may be implied (or implied), including if these additional criteria are met:

a. If it does not involve sensitive information;

b. If it does not run counter to the reasonable expectations of people in the context;

c. If no risk of serious harm emerges from the intended use or disclosure.

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

In practice, however, organizations should keep in mind that presumed consent (ATIA, s. 65.0.2; PA, s. 8.3; see paragraph 14) covers many situations in which implied consent might have been considered relevant. Cases where implied consent to a secondary purpose is actually relevant are, however, rarer.

[A priori non-compliant practice].

Example 36.1 - An elementary school offers an introductory photography activity as an extracurricular activity for fifth and sixth graders. The parents validate their children's registration by paying the appropriate fees. In November, the registered students participate in a portrait workshop and take pictures of each other. Proud of the results, the teacher in charge of the activity selects five children's photos and sends them to the school administration to be published on the school's "p arent portal", highlighting the activities of the school. and the children's progress. Both believe that parents are consenting to this diffusion since they have been informed of the portrait workshop and since the "parent portal" is secure and accessible only to parents of students. This implied 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 distribution, photos of children could be considered sensitive, and the risks of serious harm from their release should be properly assessed.
For these reasons, the school should have relied on explicit consent. It could have sent an electronic consent form to the parents concerned by 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 sent to the applicant indicates that the company will provide financing at a favorable rate for that period of time after a credit investigation by a personal information agent, whose name is listed in the e-mail. In a separate section, the email states that if the applicant does not respond, the company will provide the necessary identification information to the officer three days later. Applicant unresponsive,
the company conducts a credit check for financing, affecting his credit rating. He complains to the company that he intended to pay for the lease without obtaining financing. In this situation, the company could not rely on implied consent for the credit check request: it was contrary to the reasonable expectations of the applicant, who had not applied for financing, and
caused him significant harm by diminishing
its credit rating.

[A priori non-compliant practice].

Example 36.3 - A city council agrees to deal with questions received by e-mail from its citizens during its meetings. Citizens must identify themselves by 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 prior to posting, so names and addresses are publicly disclosed. When asked about this by a citizen, a council representative explained that it is based on implied consent, believing that people who send questions by email should reasonably expect that their contact information will be shared. However, no such information is provided on the City's website. In these circumstances, the communication may not meet the reasonable expectations of individuals and implied consent may not be valid.

[A priori non-compliant practice].

Example 36.4 - A technology start-up wants to design an artificial intelligence to assess a person's feelings based on their facial expression. To gather data to train its algorithm, it uses a data harvesting robot that scours various websites, including social networks and personal blogs, to extract photographs of
faces. The company normally requires consent for this collection from third parties. However, the company believes that by posting their photos on the web
individuals implicitly consent to their use for other purposes, including training an algorithm. This collection could run counter to the reasonable expectations of individuals, who share these photos with the idea that they will be seen by other humans they know, but not used to train artificial intelligences. Moreover, the individuals involved cannot be informed of this practice in any way, causing a transparency problem.

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

[A priori compliant practice]

Example 37.1 - A business that buys and sells auto parts wants to purchase insurance (a policy covering theft and fraud committed by employees against the business). It needs to obtain the credit report of
each employee who will be covered by the insurance policy. She consults with the employees involved to see how comfortable they are with signing up for the policy. She explains that this involves checking their credit report with their name and address once, within five business days. She asks them verbally whether or not they want to be covered by the insurance policy. This is the only question employees answer. When employees accept coverage,
since they have been adequately informed, they also implicitly consent to the
their name and address to their bank and to the collection of their
credit file with the latter.

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

39. When in doubt. If there is any doubt about the individual's wishes regarding the use or disclosure of his or her information, the organization should obtain express consent.

2.2. **Consent must be free**

40. Free character. Consent must be free, that is, it must involve genuine choice and control and be given without coercion or pressure. The person concerned must therefore be able to exercise his or her will without being unduly influenced or suffering disproportionate harm.

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 fairness of options or that influence choice therefore lead to invalid consent, since it is not truly free. For example:

a. Emphasizing opt-in rather than opt-out renders consent ineffective, regardless of exactly how it is done (visual emphasis [colors, font size, etc.], effort the user must make in number of clicks or web browsing, intentionally ambiguous wording, misleading text, etc.);

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

[A priori compliant practice]

Example 41.1 - A Municipality Makes Available an Application to Report various problems related to the maintenance of public spaces (snow removal, waste collection, etc.). To create an account, users must provide an address email address, which serves as an identifier, and a postal code 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 offers to use their email address to send them updates on the status of roadwork in their area. The agency provides an overlay window to collect this consent. The agency has the following options
The "I accept" and "I refuse" buttons are placed at exactly the same height, each in t he same color button with the same font size. By ensuring fairness in the visual presentation of choices, it ensures that the free nature of the consent obtained.

[A priori non-compliant practice].

Example 41.2 - A clothing store's Web site allows customers to create an account to facilitate their online purchases. Each time the customer logs in, a pop-up window appears offering the customer the option of receiving the newsletter weekly newsletter from the store, which includes discounts that may be of interest to them. It is as easy to accept or decline this secondary use of the email address. However, in case of refusal, the window will be displayed each time the client subsequently connects. These repeated requests for consent, regardless of the client's previously expressed wishes, may compromise the free nature of the client. 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 use and disclosure for the primary purpose if the individual provides his or her personal information on reasonable notice (ATIA, s. 65.0.2; PA, s. 8.3; see paragraph 14). When requested, therefore, it is generally for secondary purposes, which should be able to be refused without affecting the original agreement.

If the transaction 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 why the transaction is necessary in the circumstances.

[A priori compliant practice]

Example 42.1 - In the application form for student admission, a public university explains that personal information

collected will be used to assess the application, to create a permanent code and to communicate the student's status to the appropriate ministry, in the case of international students. She notes that providing the information requested on the form constitutes deemed consent to these purposes, as per section 65.0.2 of the Access Act.

In a separate section entitled "Foundation," however, the university solicits consent for a secondary purpose: "*I agree that my name, phone number, email address, date of admission, and field of study may be provided to the University Foundation for philanthropic solicitation purposes. This consent is valid for up to 5 years after my graduation. Yes - No*". The university presents this secondary purpose, which is not essential for admission, in an appropriate manner. It leaves the candidate free to to refuse the communication, without consequence on the rest of his request. This In doing so, it ensures that consent is freely given.

[A priori non-compliant practice].

Example 42.2 - When selling a new car, a dealer uses a form to obtain the information needed to provide financing to the client. In the consent section, he adds the following statement, "*By signing this agreement, I agree that my email address and name may be used to send me promotional offers for the duration of the financing.*" Asked by a customer puzzled, the business owner indicates that this modality is mandatory for receive funding. This does not deny the purpose the sending of promotional offers. Therefore, the dealer does not get a valid consent, since it is not free.

43. Changing purposes. 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 a data subject may threaten the free nature of consent. This is particularly the case in employer/employee relationships. 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 data subject is as informed as possible and that his or her other rights (complaint, access, rectification, etc.) are reserved.

[Practice may vary in compliance depending on context].

Example 44.1 - During an intervention at a food company, the inspection team of an organization with supervisory functions is photographed by his supervisor, who wishes to integrate the image into the intervention report.

The company visited has been in the spotlight for the past few months and the media has shown interest in the inspection conducted by the organization. Following a media request, the team manager sends an email to the employees who were present during the intervention to ask them if they agree that the photo in the report
The inspection report is passed on to a reporter and illustrated in the paper edition of the newspaper the next day. Given the power relationship with employees, the manager must be careful. If employees feel compelled to consent to this communication, the consent cannot be free. Therefore, the manager must be as neutral as possible in his or her request and not suggest any negative consequences to a possible refusal of communication.

[A priori compliant practice]

Example 44.2 - A Hospital Decides to Implement an Access Control System
biometric to restrict access to a room where a machine is located that operates with a highly radioactive material. Nuclear safety agency standards require particularly strong security to limit the risk of theft or sabotage of such material. Upon completion of the Privacy Impact Assessment, the Freedom of Information and Protection of Privacy Committee
The organization's personnel department approves the acquisition of a biometric system and declares the creation of a biometric 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 be required to present a
and then validate their identity with a security guard. Both the cards
The hospital has made reasonable efforts to ensure that all biometric and traditional access information remains under the control of the individuals concerned. In these circumstances, the hospital has made reasonable efforts to
preserve freedom of consent, despite the employment context: employees

45. Link to granularity. Consent is free only if requested separately for each purpose (granularity; see section 2.5). The data subject should not have the sole choice of accepting or refusing everything.

46. Withdrawal of consent. Free consent is also consent that can be withdrawn at any time by the person concerned. Although consent is presumed in some cases (ATIA, s. 65.0.2; PA, s. 8.3) and therefore has not been assessed as free, it may still be withdrawn as provided for in the legislation (ATIA, s. 65; PA, 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 implications for the free nature of the consent.

[A priori compliant practice]

Example 46.1 - A team in a university research laboratory is conducting a study on voice perception. To build up their material, they recruit participants to be recorded while they recite a text. They sign a
consent including all required information and allowing researchers to reuse the voice in further studies on the same subject during
five years. Participants who, at some point, would no longer like their voice to be

used by the laboratory can withdraw their consent by sending a simple email to the p rincipal 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. An overlay window that appears when they first log in allows them to activate personalized recommendations to discover music. An algorithm then draws up their profile based on the songs they listen to, the length of time they have been listening to them, etc.
and the time of day during which the listening is done. Believing that these recommendations prevent him from discovering music on his own by exploring the platform, a user decides to withdraw his consent to the use of this information for personalized recommendation purposes. He has to make eight clicks in the different settings screens of the application before finding the option to disable the function. While it only takes one click to consent to
personalized recommendations, it takes a lot more to withdraw consent.
In the context, these 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 individual 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. Capacity of the person. To be informed, consent must first be given by a person who is capable of obliging himself or herself at the time he or she gives it (*Civil Code of Quebec*, article 1398). For example, consent given by a person who is incapable or under 14 years of age (ATI, sections 53.1 and 64.1; LP, sections 4.1 and 14) is not valid. In these circumstances, however, it may be given by a representative, such as a parent or guardian.

49. Information to be provided. In order to understand what consent is being sought, the individual must be able to access the following information (in many cases similar to what organizations are required to provide at the time of collection of personal information [ATIA, s. 65; PA, s. 8]) :

a. **Who?** Organization on whose behalf the consent is sought;

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

c. **To whom?** If applicable, name(s) of third party(ies) or class of third party(ies), outside the organization, to whom the organization will share the information;

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

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

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

g. **Until when?** Duration of validity of consent (see section 2.7);

h. **What if I don't?** Consequences of not consenting or withdrawing consent later (the organization must ensure that they do not compromise the free nature of the consent).

i. **With what risks?** Reasonably foreseeable risks or consequences associated with the transaction to which the consent relates, if applicable;

j. **How is it used?** Means of using or disclosing the information (e.g., postal communication; use of fully automated decision making);

k. **Where will the information be disclosed or stored?** The location where the information will be disclosed or stored in connection with the transaction to which the consent relates, specifying whether there is a possibility that the location will 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 departmental employee has an individual sign a generic consent form before completing all the fields. The text presented to her reads as follows, with no information on the blank lines:
"*I authorize the Department to release the following information:*
_____*to the following persons :* _____
. and for the following purposes : _____. " This does not does not allow for informed consent. The person cannot understand the scope of what they are agreeing to if they have no information as to what is intended by that consent. At the time consent is sought, it must be possible to given with full knowledge of the facts.

[Practice may vary in compliance depending on context].

Example 49.2 - Two online shopping platforms collect consent from buyers to communicate their contact information to other companies so that they 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 to send me promotional offers.*"

Platform B's more complete text is 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 give any indication of the identity of its partners.

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

a. **First level**: immediately and effortlessly accessible information directly in the consent form.

   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, as well as the **information or categories of information involved** (what), whenever possible. Elements that may be surprising to the data subject should also be included (e.g., long shelf life, use of an unusual technology, numerous or significant risks, etc.);

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

   i. A privacy policy that is accessible through a prominent link, including where technology is used (ATIA, section 63.4; PA, section 8.2);

   ii. An appendix to a form;

   iii. A question mark icon or "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 involving to work 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 applicant 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 release of the clearance certificate to the SSC criminal history record that has been created. To ensure that this consent is informed, the SSC uses the following text, which captures the essential information from the consent application:

> *"SSC X* [who?] *needs your consent to release your identity information* [what?] *to Police Department Y* [to whom?
> *conduct a background search to certify that you can work with vulnerable persons* [why?] *This consent also covers the release of the certificate of absence to SSC X by Police Department Y*
> *criminal record* [what?]*. It is valid only until the certificate is actually transmitted* [until when?]*. If you refuse, we will not be able to*

not proceed with your application [and if not?] *Additional information is available i n Appendix A.*

☐ *I accept* / ☐ *I decline*."

Appendix A provides the rest of the information, such as the right to withdraw one's 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 shall state the purpose of the consent and the categories of information to which it applies. The consent is valid for the duration of the next fiscal year. It also includes a link to a privacy policy. When the user clicks on this link, a pop-up window displays a simple policy with additional information (technical means of processing the information, location of storage, risks, explanation of the right to withdraw consent, right of access and right of rectification, and contact information for 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 overloading the consent request. The consent obtained is therefore informed.

51. Precision and clarity of terms. The elements presented above should allow for specific consent (see section 2.4) 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 people to understand what they are agreeing to.

52. Separate information for each purpose. When a request for consent to secondary use or disclosure is made at the time of collection of 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 (ATIA, Sections 65 and 65.0.1; PA, Sections 8 and 8.1);

b. Information about other purposes for which consent is sought. However, this must be done separately (see section 2.5, and section 2.8 for written requests). There is thus a link between the informed nature of consent and the amount of information given to the data subject at the same time: 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, the persons to whom the complaint must be communicated in order to ensure that it is processed in accordance with the policy, and the mandatory nature of the information required to process the complaint (with the exception of the first and last names, which are requested on an optional basis). The rights of access and rectification are also presented. At the end of the form, once the person reporting presses
"*Next*," the university provides a separate page requesting consent to allow the complaint handling office to discuss the complaint with the appropriate department chair. It provides specific information regarding this consent. Providing the new information separately from the information about the collection of information necessary to process the complaint, the university promotes informed consent to disclosure.

53. **Subsequent availability of information.** Since free consent can be withdrawn, the data subject must have access to relevant information even after consent has been given, so that he or she can reassess the decision if necessary. Thus, an organization must deploy means to make information readily available.

54. **Duty to assist.** An organization shall provide assistance to individuals seeking 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 access the online services of an organization that uses a third party authentication service, an individual must consent to the
The third party may provide certain identifying information 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 for assistance in understanding the consent being sought. It also offers to speak with an agent over the phone by providing a toll-free number that is accessible during business hours. These mechanisms make
part of the tools deployed by the organization to provide assistance to those in need.

2.4. **Consent must be specific**

55. **Specificity.** Consent must be given for a specific purpose, i.e., it must have a precise and circumscribed object. This criterion is closely linked to that of informed consent: a person can only consent if he or she is able to understand exactly what is being asked of him or her.

56. **Specificity of 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 consent, and therefore its validity.

[A priori non-compliant practice].

Example 56.1 - A school obtains parental consent for the team to
multidisciplinary team can share information about the child's progress

to a health care facility where he has recently been receiving additional services. She asks them to consent to "*any information deemed necessary*" being
The term "*may*" *be* communicated to "*any other person who needs it*". The use of these imprecise terms compromises the informed nature of parental consent, as well as its specificity. The school should specify the specific purpose(s) intended, which in this case is to provide better support
The school should also specify the information to be disclosed and the anticipated frequency of disclosure, as well as the intended categories of recipients (e.g., "professionals involved in the child's care at the school"). The school should also provide details about the information involved and the anticipated frequency of disclosure, as well as specify the intended categories of recipients (e.g., "*the professionals assigned to monitor the child at health care facility X").*

[A priori non-compliant practice].

Example 56.2 - A union seeks express consent from some of its members to use some of the personal information contained in active grievances to "*improve its processes*. This term is impr ecise and undermines the specificity of the consent, as it does not provide a clear understanding of t he purpose. The purpose should be more clearly stated
(e.g., "*staff training*"),
"training of an artificial intelligence to automate certain steps of the processing the grievance", etc.).

57. Limiting use. In order to respect the specific wishes of data subjects, 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 an organization makes an unintended use or disclosure of information that is not consistent with what individuals consented to or with the purposes identified at the time of collection (unless the legislation provides an exception, such as consistent purposes), is a privacy risk and a privacy incident (see paragraph 16).

[A priori non-compliant practice].

Example 57.1 - An intermunicipal board is asked by a company to provide the last year's attendance record of one of its employees who wishes to obtain a position with 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 sent the employee's *complete* attendance record, which covered four years of service. In doing so, it did not respect the specific consent that had been obtained, which related exclusively to the disclosure of the attendance record of the last
year.

[A priori non-compliant practice].

Example 57.2 - An individual who purchases a television and a computer online consents to the retailer sharing his contact information and purchase information with three partner companies, explicitly 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 their

aprovides the information. However, he or she cannot do so under the original consent given, since the consent was specifically directed to the partners precedents.

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

2.5. **Consent must be granular: each of the 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 ensure that the purpose of consent is as narrow as possible, at the level of the purpose. In other words, if there are multiple purposes, it should provide 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 choice is to refuse or accept as a whole, which does not represent all the nuances of the individual's wishes. 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 that funds projects collects applications through a form. It wishes to seek consent for two purposes: (a) to provide the applicant's contact information to a broadcaster for the purpose of promoting the successful projects, and (b) to use the e-mail address for the purpose of sending a survey. It provides a "consent" section, where these two requests are made in succession, and then adds a single box
The organization asks for one "*I agree" box* and one "*I decline"* box. By doing so, the organization compromises the granularity of consent by asking for one authorization for two purposes. It should be possible for an individual to consent to the release 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 not-for-profit organization holds a gala event to award
awards recognizing the work of specific practitioners in its field. It collects email addresses from nominees to inform them of their nomination and details of the ceremony. It also asks nominees to consent to three secondary purposes: a) to use their email address to contact them to evaluate their
b) use their email address to send them the organization's general newsletter; c) allow the company designated by the organization to take the official photos of the winners to keep their email address on file for future reference.
offer them discounts on other photography services. In order to respect the

granularity of consent, the NPC arranges these three purposes in a table with a "Yes" column and a "No" column to allow applicants to accept or decline each of these three purposes separately:

"Consent. Do you consent to your address being :

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

  ☐ Yes ☐ No

- *Used to send you our general newsletter?*

  ☐ Yes ☐ No

- *Retained by the company designated to take official photos of the to offer you discounts on other services?*

  ☐ Yes ☐ No "

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

61. Understandability. The request for consent must be understandable, i.e., presented in simple and clear terms, both in terms of the information and the specific statement of acceptance or refusal. This criterion is intended to ensure 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 a number of elements that can simplify and clarify statements for individuals, including those discussed in the following paragraphs[4] .

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 many periphrases. Overly long sentences or texts are detrimental to the understanding of the people involved.

[A priori compliant practice]

Example 62.1 - In a consent form for assistance a department uses the following formula: "*I authorize the department t o provide as soon as possible to the rehabilitation service provider information related to holding an account with a financial institution all of theto for proceed, if necessary, with the payment of my financial assistance*."

When it comes time to completely revise his form, he changes it to the following: *"I authorize the Departmetransmit at the rehabilitation the contact details my bank account in order to disburse my financial aid*".

It improves conciseness and clarity without losing crucial information.

[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.

63. Simplicity of vocabulary. An organization should use simple terms that are accessible to those involved. 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 of their purchases. 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 their profile
of buyer, which it wishes to determine from their transactional history. To do this, it seeks the consent of the users of the application by the following text:

> *"Receive Personalized Offers - By checking "Yes", the Customer consents to the automated analysis by the Company of historical transactional data for the purpose of determining a profile by machine learning model; said profile will be used by the Company to*
> *Issue, but not formally commit to, and subject to its existing policies and procedures, personalized offers of discounts on the purchase price of certain products, provided the Customer complies with the terms of use."*

This very legal style text contains several words that are not common vocabulary and several complex turns of phrase (long sentence, incises, etc.). It can confuse the person 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 comply with the terms and conditions*
> *loyalty application usage. ☐ Yes ☐ No* "

64. Clarity of intent. An organization should use the most direct terms possible to ask the individual for permission, both in the way it is presented and in the wording of the options available to the individual. The use of precise language avoids confusion about what the individual is 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 it is unavoidable to use it.

[A priori compliant practice]

Example 64.1 - An organization reviews its procedures for obtaining consent, according to a schedule defined in its governance rules. The committee formed for this purpose notes that requests for consent are generally introduced by language referring to knowledge rather than authorization: "I am *aware* that information X will be used [...]" or "I *understand* that information Y will be disclosed to [...]".

In order to clarify them, he 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, on web interfaces, the explicit consent options also do not reflect the consent situation (opt-in or opt-out). In many cases, the options offered are "*Next*" or "*Ignore,*" while in other cases, the wording of the options emphasizes acceptance over refusal. For example, a consent overlay window offers users the option of pressing "*Yes!*" or "*Maybe later.*" At the recommendation of its committee, the organization is homogenizing the options to present a choice between "*Yes*" and "*No*" as often as possible, or, alternatively, "*I agree/I consent/I agree*" and "*I refuse/I do not consent/I do not agree.*"

Through these changes, the organization is moving toward clearer and simpler language and
promotes informed and free consent.

65. Tailoring to the audience. Information should be tailored to the intended audience. An organization needs to consider the perspective and profile of the individuals to whom the information is directed: they may not have a background in their privacy rights or knowledge of the organization's activities, and some may not be fluent in either oral or written language. The organization should also tailor the language used to the lowest level of literacy among the different categories of data subjects to whom a consent request is directed.

[A priori compliant practice]

Example 65.1 - At the request of an Aboriginal nation that is intensifying its efforts to revitalize its language, a team of researchers is conducting an in-depth linguistic study with the elders of the nation, in partnership with an Aboriginal 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.). Participants are asked to tell a traditional story. The cultural institute would like to ask participants to agree that recordings of these stories can also be posted on a section of its website dedicated to the nation's language and the preservation of its intangible cultural heritage. He uses a French form to do this. Some of the older participants speak very little French. To ensure that the consent form is adapted to them and that it is understandable to them, the cultural institute mandates a bilingual agent to collect oral consent from these participants and
to answer their questions, if needed.

[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, it conducts
understanding with approximately 100 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 clients. In this way, the company ensures that the terms are simple and clear for the people concerned.

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

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

67. Term Limits. The term limit can be linked to two types of conditions:

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

b. **An event**: the purpose can be considered accomplished 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 consulted to learn about the candidate's work in previous positions, in addition to the information on the evaluations in the candidate's file. 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 specificity and informedness. In order to be able to provide specific and informed consent, data subjects must be informed of the duration of their consent. Again, vague or imprecise language should be avoided. If the end of consent is linked to an event, an organization should provide sufficient information to the data subject 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).

69. Transparency in relation to long-term consents. Where an organization seeks consent for a very long time, it should pay particular attention to transparency on an ongoing basis. It could remind individuals at appropriate intervals that it is using or disclosing 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.

[5] CAI is not responsible for enforcing this law.

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

70. Separateness. If the request for consent is made in writing, it must be presented separately from any other information. It is therefore separate from terms of use, broader privacy policies, requests to confirm the validity of information provided, commitments, signatures, etc. It must be featured in its own section or interface (form section, overlay window in an application, etc.), so it is easily accessible to the person concerned.

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

a. **Overt and free**: consent is not overt if it is expressed by an action that may also be evidence of something else, such as the receipt of information or the validity of the information provided, since the intentions behind the action 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 requests for consent help to limit the amount of information provided at one 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 for a professional order, the individuals involved must sign after four statements:

> *"I acknowledge that I have read the instructions [...].*
> *2. I declare that the information provided is complete and accurate [...].*
> *3. I agree that the College may release 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 is included among three other statements that are not consents. This also compromises the clear and free nature of the consent. To correct this, the College 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 College sharing my information with the group insurer [...].*
>
> ☐ *Yes* ☐ *No*
>
> *By signing this form :*
> ✓ *I acknowledge having read the instructions [...].*
> ✓ *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 an account creation 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. No reference to consent is included in the form, however. By clicking on the link, a player can discover
that the terms of use contain, among other things, the privacy policy of the publisher. It is mentioned in the text that by accepting the terms of use, the player consents to the use of his friends list, metadata on his device, his interactions with the game (clicks, times, etc.) and his conversations on the public server for the purpose of targeted advertising, improving the game experience and fighting
against cheating, among other things. The player also agrees to the publication of his score in the game on a public platform, along with his nickname and game history, 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 and conditions of use that address a variety of other matters undermines the distinctiveness of consent. Moreover, this situation threatens its manifest character (gesture of
consent inseparable from the act of accepting the terms of use), free
(granular refusal impossible) and informed (information difficult to access).