



Guidelines 2023-1

Consent: validity criteria

Version 1.0

October 31, 2023

The Commission d'accès à l'information ("CAI") has confirmed that it will not be publishing an English version of its "Lignes directrices 2023-1 – Consentement: critères de validité". Considering the interest of organizations and individuals throughout Canada for Québec's amendments to its private sector act, BLG has made available this unofficial translation to facilitate understanding of these guidelines. Readers should refer to this translation with care and review the original French version published by the CAI. In the event of a discrepancy between the original French version and this unofficial translation to English, the French version shall take precedence.

Summary of the guidelines

Who are these guidelines for?

These guidelines are intended for public and private organizations that need to obtain consent from individuals to use or disclose their personal information.

The objectives of these guidelines

- ✓ Facilitate understanding of the criteria to be met in order to obtain valid consent;
- ✓ Clarify the obligations of organizations in obtaining valid consent;
- ✓ Identify good practices that promote respect for individuals' right to privacy.

What is excluded from these guidelines

- ✗ Consent to the disclosure of non-personal information, such as technical and financial information or trade-secret;
- ✗ Detailed explanation of when organizations must obtain consent;
- ✗ Exceptions allowing the use or disclosure of personal information without consent. In this case, the validity criteria are irrelevant.

What do the guidelines contain?

- A glossary of key concepts
- An introduction to consent and the obligations of organizations
- A detailed explanation of the 8 criteria for valid consent
- Examples to help understand the criteria

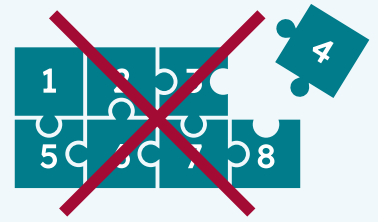
Laws and regulations take precedence over these guidelines

In case of doubt or conflict with these guidelines, laws and regulations always take precedence.

Consent gives individuals control over their personal information

By default, personal information is confidential in order to protect the privacy of individuals. Consent gives individuals control over the use and disclosure of their personal information. This implies that they agree to what is done with their information.

For their part, organizations must comply with their legal obligations to protect personal information. This includes the obligation to obtain valid consent from the persons concerned. Organizations should document this consent and the elements that support its validity.



The 8 criteria for valid consent

To obtain valid consent, organizations must ensure that it complies with 8 criteria listed in the law. The 8 criteria are interrelated and all important. If a criterion is not met, consent is not valid.

- 1** Consent must be **clear**, i.e. obvious, and provided in a way that demonstrates the true will of the person concerned. In most cases, this will should be express, i.e. given by a positive statement or gesture that indicates consent alone, though it may be implicit in certain circumstances.
- 2** Consent must be **free**, that is, it must involve real choice and control, and it must be given without coercion or pressure. It must be as easy to provide one's consent as it is to decline providing it. The person concerned must also be able to withdraw consent at any time.
- 3** Consent must be **informed**. The person concerned must understand what he or she is consenting to and what this entails. The organization requesting consent must provide precise information. Among other things, it should mention the purpose for which the information is being collected, what information is being collected, and who will have access to it. Lastly, the person giving consent must have the capacity to do so (e.g. not be an incapacitated person or a person under the age of 14).
- 4** Consent must be given for **specific purposes**. In other words, the purposes for which personal information is used or disclosed must be as specific as possible.
- 5** Consent must be **granular**, that is, it must be requested for each purpose described. If there is more than one purposes, consent must be asked separately for each of them. This granularity allows the person concerned to express his or her wishes clearly, as he or she can accept or refuse each specific purpose.
- 6** The request for consent must be **comprehensible** (or understandable), i.e. presented in clear and simple terms, both in terms of information provided and specific inclusion of a statement of acceptance or refusal. Information presented should be concise, that is to say, it should be expressed with a minimal number of words. An organization should avoid unnecessary and complex words (legal jargon). Terms should be as direct as possible.
- 7** Consent must be **temporary**, i.e., it must be valid for a limited period of time. It shall be valid only for the period which is necessary to achieve the purposes for which it was requested. The duration limit can be linked with a time limit (e.g. 6 months or 3 years) or an event (e.g. as soon as a payment is made).
- 8** If a request for consent is made in writing, it must be **made separately from the provision of any other information**. It must therefore be separate from the terms of use, privacy policies, signatures, etc. The request for consent must be featured in its own section or on its own interface and be easily accessible to the persons concerned.

Warning

Personal information must be necessary

By law, personal information must be necessary for the fulfillment of an organization's purposes. This is true at every stage of the personal information life cycle: collection, use, disclosure, retention and destruction. The consent of an individual does not authorize an operation to be carried out with personal information that is not necessary.

Personal information must be protected

After obtaining valid consent, organizations are responsible for protecting the personal information they hold.

Table of Contents

Glossary	1
Introduction	2
A. These guidelines aim to clarify the criteria for valid consent	2
B. Consent gives individuals control over their personal information	3
C. It is essential that organizations document their practices	6
Criteria for valid consent	7
1. Consent must be clear	8
2. Consent must be free	10
3. Consent must be informed	12
4. Consent must be specific	15
5. Consent must be granular: it is required for each purpose targeted	16
6. A request for consent must be understandable: it must be presented in clear and simple terms	17
7. Consent must be temporary: it must be valid only for the duration for which it is necessary	18
8. A request for consent shall be separate: it shall be submitted separately if it is in writing	19
Examples	20
D. Examples related to the introduction	20
E. Examples related to clear consent	22
F. Examples related to free consent	25
G. Examples related to informed consent	28
H. Examples in relation to the specific character of consent	31
I. Examples related to the granular character of consent	32
J. Examples related to the comprehensible character of consent	33
K. Examples related to the temporary nature of consent	35
L. Examples related to the distinct nature of consent	35

Glossary

In this document, certain simplified terms are used to refer to more complex legal concepts:

Information refers to personal information, i.e. any information which relates to a natural person and directly or indirectly allows that person to be identified.

- For example, a postal or e-mail address, a unique number, geolocalization data, a photograph, a psychological characteristic, etc.

Sensitive information refers to personal information that, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy.

- For example, a fingerprint, a notice of assessment number, a diagnosis, etc.

Organization refers to any entity, public or private, to which section 53.1 of the *Act respecting access to documents held by public bodies and the protection of personal information* or section 14 of the *Act respecting the protection of personal information in the private sector* applies.

Primary purposes refer to the purposes for which personal information is collected by an organization. They relate to the provision of a service or product, or access to employment. They are disclosed at the time of collection.

- For example, to process a customer's payment, a company collects financial information; to process an application for benefits, a public body collects information about a person's employment.

Secondary purposes refer to all other purposes pursued by an organization.

- For example, to carry out a market study, a company wishes to reuse information it already has; to facilitate administrative procedures with another organization, an organization wishes to communicate information about a citizen's file.

Introduction

A. These guidelines aim to clarify the criteria for valid consent

A.1. Purpose of the guidelines

These guidelines address the **criteria for valid consent** that organizations must obtain from the individuals whose personal information is concerned.

These criteria are set out in:

- a. Section 53.1 of the *Act respecting access to documents held by public bodies and the protection of personal information* (the “**Access Act**”);
- b. Section 14 of the *Act respecting the protection of personal information in the private sector* (the “**Private Sector Act**”).

Unless other provisions are explicitly mentioned in this document, in which case they will be referenced at the bottom of the page, the guidelines are exclusively aimed at the interpretation of these two provisions.

A.2. Intent and significance of the guidelines

The *Commission d'accès à l'information* (the “**CAI**”) is disseminating these guidelines in order to facilitate the application of the Access Act and the Private Sector Act, the laws for which it is responsible¹. The purpose of this document is to clarify the obligations of organizations with regard to obtaining valid consent, taking into account the legislation as a whole and case law.

The guidelines do not have the force of law. Laws and regulations take precedence at all times.

A.3. Obligations and good practices

These guidelines also identify good practices that promote respect for individuals' right to privacy. The CAI distinguishes these from obligations throughout the text:

- a. When referring to **obligations**, it mainly uses the verb “must” in the present tense (“must”, “shall”);
- b. When it urges the adoption of **good practices**, it uses the **conditional tense or terms related to recommendation or possibility** (“should”, “could”).

A.4. Exclusions

These guidelines do not address consent to the disclosure of *non-personal* information - such as technical or financial information, or trade-secret².

Nor are they intended to provide specific guidance on situations where consent is or is not required, except general information in [Section B](#) that focuses on the criteria which must be met when consent is required by law.

1 Access Act, section 123.

2 Access Act, section 23, section 25, and section 49.

A.5. Examples

Examples are given in the second part of this document to illustrate the content of these guidelines. The examples are fictitious but may be based on actual practice. They are simplified to highlight specific consent issues and thus illustrate a specific aspect of the text (for example, a single validity criterion). In practice, every situation requires its own specific analysis. These examples are therefore tools. When a potentially non-compliant situation is described, the CAI suggests a course of action, but this should not be regarded as the only possible solution.

Although the examples are generally associated with a sector, public or private, they may inspire organizations in the other. The following icons and colors are used to classify them:



A.6. Other laws

Organizations are responsible for knowing and complying with their consent obligations under other sectoral legislation, such as the *Act Respecting Health and Social Services*, or general, such as the *Civil Code of Quebec*. In addition, obtaining valid consent does not negate the organizations' other legal obligations to protect personal information.

B. Consent gives individuals control over their personal information

B.1. Right to privacy and control

Individuals have a fundamental right to privacy. By default, personal information is therefore confidential. Everyone has the right to control the collection, use and disclosure of their personal information.

B.2. Control procedures

The law provides for this control to be exercised:

- a. Through rights (access, rectification, etc.) or remedies (complaint to an organization or the CAI, etc.). To ensure that people can exercise these rights with full knowledge of the facts, the law lays down **transparency** obligations for organizations;
- b. Through **consent**. Linked to personal autonomy, consent implies that individuals give their assent to certain actions involving their information. To be legally **valid**, consent **must** meet certain criteria (see [page 7](#)).

B.3. Consent and collection

Unlike other Canadian or international privacy laws, the Access Act and the Private Sector Act do not provide a framework for collecting information through consent, except in specific cases. Instead, to **collect** personal information, an organization **must**:

- Clearly identify the purposes for which the information is collected, and meet the **necessity** threshold³;
 - i. In particular, the purposes must be important, legitimate and real. The collection must be proportional to these purposes, i.e. rationally linked to them, limited to the maximum, and clearly more useful to the organization than harmful to the individuals concerned;

3 Access Act, section 64; Private Sector Act, section 5.

- Respect its **transparency obligation** by providing accurate and complete information to data subjects when data is collected from them⁴.

B.4. Collection involving technological functions

When an organization collects information using technology whose functions permit the identification, localization or profiling of an individual, these functions **must** be disabled by default⁵. The law also imposes an additional obligation of transparency. The organization **must** inform persons concerned of the following:

- The fact that it uses such technology;
- The means available to activate identification, localization or profiling functions. The person concerned must therefore take positive action to do so.

See examples [B-a](#) and [B-b](#)

B.5. Special circumstances

In special circumstances, an organization **must** obtain valid consent to :

- a. The collection of personal information **from a minor under the age of 14**⁶;
- b. The collection of information **from a third party** rather than from the individual concerned, except in the private sector⁷.

B.6. Consent and primary purposes

An organization that duly respects its transparency obligation when collecting personal information from data subjects may consider that those who provide their information with full knowledge of the facts consent to the use and communication necessary for the primary purposes announced⁸. This consent may be withdrawn at a later date (see [section 2.3](#) and [section 2.6](#)).

B.7. Consent and secondary purposes

Subject to certain exceptions, an organization **must** obtain valid consent to:

- **Use** information for secondary purposes⁹;
- **Disclose** information to a third party¹⁰.

See example [B-c](#)

B.8. Consent and necessity

Consent never allows the requirement of **necessity** to be waived. (see [section B.3](#)). Thus, at all stages of the lifecycle of personal information, including during collection, use, disclosure, retention and destruction, the information **must** be necessary for the purpose for which it is to be used. This requirement is well established in laws¹¹ and case law.

4 Access Act, section 65 ss.; Private Sector Act, section 8 ss.

5 Access Act, section 65.0.1; Private Sector Act, section 8.1.

6 Access Act, section 64.1; Private Sector Act, section 4.1.

7 Private Sector Act, section 6.

8 Access Act, section 65.0.2; Private Sector Act, section 8.3.

9 Access Act, section 65.1; Private Sector Act, section 12.

10 Access Act, section 53, section 59, and section 88; Private Sector Act, section 13 and section 40.

11 For instance, Access Act, section 64, section 65.1, and section 67; Private Sector Act, section 5, section 12, and section 18.

B.9. Time of consent

An organization **must** obtain consent **before** performing actions for which the consent was obtained to achieve.

B.10. Exceptions to consent

In some cases, the Access Act and Private Sector Act provide for exceptions that allow an organization to use or disclose personal information without consent. Many other statutes also provide for similar exceptions. Where such an exception applies, the validity criteria (see [page 7](#)) are not applicable, since there is no requirement to obtain consent.

B.11. Transparency

An organization **should** demonstrate transparency by describing, in one of its publicly available documents¹², the exceptions to consent it is most likely intending to avail itself of. This practice ensures that individuals are informed of these possibilities and can exercise control over one's own personal information, through their rights and recourses (see [section B.1](#)).

B.12. Use of exceptions

To benefit from a consent exception, an organization **must** ensure that the relevant conditions are met.

Exceptions are, however, optional. Organizations **should** only use them if it is not possible or appropriate to obtain consent. In certain cases, organizations **can** therefore opt to rely on consent instead, especially when obtaining consent poses no practical difficulties (easy-to-reach people, non-urgent situation, etc.).

The following elements may be considered as part of an organization's analysis of whether it opts to rely on exceptions to consent for some of its activities:

- a. Relying on consent may sometimes be more beneficial to the organization, for example to facilitate demonstrable compliance (see [section C](#));
- b. Consent can also be later withdrawn by an individual (see [section 2.6](#)), providing an additional means of control over one's own personal information;
- c. The organization may wish to improve transparency in the management of personal information.

B.13. Respect the choice of individuals

Consent must allow genuine control of the persons concerned. If, for a specific purpose, an organization chooses to rely on consent rather than an applicable exception for the collection, use or disclosure of personal information, it **should** respect the choice of the individuals involved. Thus, it **should not**, when an individual refuses to consent or withdraws their consent, instead choose to rely on for the same purposes.

B.14. In case of doubt

If an organization is uncertain or cannot demonstrate that an exception applies in a given situation, it **must** instead obtain the valid consent of the person concerned.

¹² These may include, for example, governance policies or rules, or a privacy policy, depending on the circumstances.

C. It is essential that organizations document their practices

C.1. Importance of documentation

The CAI stresses the importance of documenting organizations' consent practices. Organizations **should** carefully consider this issue. Documentation helps structure considerations about the protection of personal information. It allows organizations to better justify their actions in the event of a complaint, an allegation, or an investigation. When the validity or obtention of consent is inadequately documented, there is a risk that the CAI or any court may find that consent was not valid or was not obtained in a given situation. This could result in a violation of the law.

C.2. Documentation of the obtention of consent

Where consent is required, an organization **should** document that it has been obtained (or withdrawn; see [section 2.6](#)). However, documenting evidence of consent **should not** require collecting more information than is necessary. It **should** develop and implement methods that are appropriate to their contexts and activities, and the form of consent (see [section 1.2](#) and [section 1.3](#)).

See example [C-a](#)

C.3. Documentation of the validity of consent

A consent that does not satisfy the validity criteria is without effect¹³. In the same vein, organizations **should** document elements to demonstrate the validity of consent. Once again, it is up to the organization to determine the best means of doing so. This **may** involve, for example, retaining factual elements related to the request for consent or the elements to demonstrate that the obligation to obtain valid consent was previously fulfilled (information provided upfront, script used by the organization's agents on the telephone, etc.) Such documentation makes it easier to attest, at a later date, that a practice was compliant at the time consent was obtained.

See examples [C-a](#) and [C-b](#).

C.4. Authentication of the person concerned

Since consent is an expression of personal will, an organization **must** ensure that it obtains the consent of the person concerned themselves, or their legal representative, where applicable. (see [section 3.2](#)). Where there is a legal representative, the organization **must** also verify the capacity of the consenting person (i.e. the holder of parental authority, the legatee, the representative, etc.) This **may** include validating certain personal information, but the organization **must not** retain or collect more information than is necessary. The organization **should** aim for a reasonable degree of certainty depending on the context of its activities, taking into account, among other things, the purposes for which the information is collected, the sensitivity of the information and the nature of its activities.

¹³ Access Act, section 53.1; Private Sector Act, section 14.

Criteria for valid consent

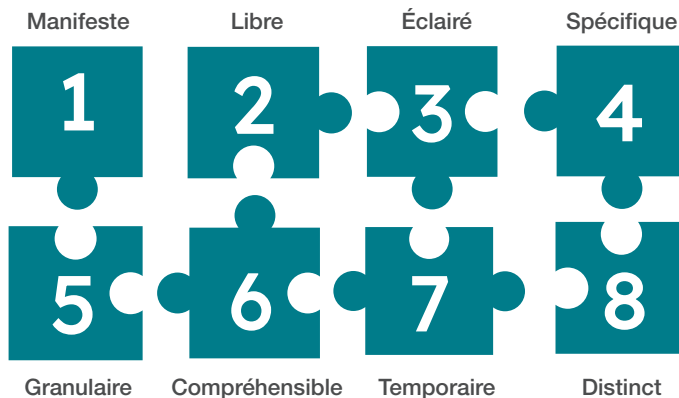
Valid consent is defined in sections [53.1](#) of the Access Act and [14](#) of the Private Sector Act, which both contain eight criteria (each box in the text is a link to a specific section of these guidelines):

“Consent [under the law] must be **clear, free** and **informed** and be given **for specific purposes**. It must be requested for each such purpose, **in clear and simple language**. When the request for consent is made in writing, it must be **presented separately** from any other information provided to the person concerned. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.

[...]

Consent **is valid only for the time necessary to achieve the purposes** for which it was requested.”

“Consent not given in accordance with [the law] is without effect.”



The first four criteria (clear, free, informed, specific) are fundamental, while the subsequent four (granular, comprehensible, temporary, distinct) relate to particular aspects of the first four and ensure their complete validity. For example, requests for consent must be presented in simple and clear terms to be considered as being informed and specific. **As the text progresses, the links between the criteria are clarified when relevant.**



1

Consent must be clear

1.1. Clear consent

Consent **must** first and foremost be **clear**, i.e. obvious, and provided in a way that demonstrates the true will of the person concerned. In most cases, this will should be **express**, though it may be **implied** in certain circumstances.

1.2. Express consent

Consent is **express** when the individual takes an active step (or makes a statement) that clearly indicates their consent. Such a gesture or declaration therefore serves no purpose other than to provide consent and is considered to be **positive**: it indicates acceptance, not refusal. Accordingly, there is no doubt as to the true will of the individual. The expression **opt in** also refers to this form of consent.

1.3. Implied consent

Consent is **implied** if it is not expressly stated. Rather, the organization deduces it from a separate, unrelated action taken by the person concerned, or from the silence or inactivity of the person concerned. The person concerned **must** be informed that this action, silence or inactivity will be interpreted as consent (see [section 3](#)). He or she **should** have a valid opportunity to withhold consent. This form of consent is also referred to as **opt-out**.



1.4. Methods of consent obtention

An organization is free to develop mechanisms which allow for the obtention of express consent, so long the mechanisms are appropriate given the organization's activities, and as long as the mechanisms are compliant with the law. These mechanisms **should** be tailored to the individuals involved, and to the context and the type of interface used. Below are some examples based on the form of consent:

a. Express consent

- i. Signing a document;
- ii. Ticking a box;
- iii. Answering a question in the affirmative;
- iv. Verbal approval.

b. Implied consent

- i. Use of pre-checked boxes;
- ii. Deduction related to the person's silence or inactivity;
- iii. Deduction related to a separate act of the person.

See examples [1-a,1-b](#) and [1-c](#).



1.5. Selection of express or implied consent

In some situations, express consent is required. In other, the organization determines whether express or implied consent is best suited to its activities. The elements presented in the following sections are intended to guide the analysis to be carried out.

1.6. General guidelines

Express consent is **mandatory** when an organization wishes to use or disclose **sensitive information**¹⁴. However, consent is not required for the use or disclosure of sensitive information for the primary purposes for which it is collected¹⁵ (see [section B.6](#)) It should be noted that other laws in Quebec require express consent in certain situations.

Since it does not require an active, positive gesture, implied consent **should** only be used when the following additional criteria are met if:

- a. The use or disclosure does not conflict with the **reasonable expectations** of individuals in the context;
- b. No **risk of serious harm** emerges from the intended use or disclosure.

Consent to the use or disclosure necessary for the primary purpose (see [section B.6](#)) includes many situations in which implied consent might have otherwise been considered relevant. Cases where implied consent to a secondary purpose is relevant are rare.

See examples [1-d](#), [1-e](#), [1-f](#), [1-g](#) and [1-h](#)

1.7. Compliance with all criteria and documentation

Whether consent is express or implied, it **must** be clear, i.e. evident from the individual's behavior. The organization **must** also ensure that the other criteria for valid consent are met. Since express consent is formally requested, it facilitates compliance with some of these criteria, such as granularity (see [section 5](#)), comprehensibility (see [section 6](#)) and distinctiveness (see [section 8](#)). It is also easier to document (see [section C](#)) and leaves no doubt as to the true will of the person concerned. For these reasons, organizations **should** prioritize express consent.

1.8. Consent fatigue

Even if it opts for express consent, an organization **should** take steps to mitigate consent fatigue. Indeed, every day, we are asked to provide consent in a multitude of contexts. In the digital world, this is often done by ticking a box or clicking a button. Although the repetitive nature of these actions may render them less meaningful, it is still important for the persons concerned to be aware that they are providing consent. This, particularly to ensure that they understand the information made available to them (informed consent criterion; see [section 2.3](#)).

1.9. In case of doubt

If there is any doubt as to whether the individual really consents to the usage or disclosure of their information, the organization **should** obtain express consent.

¹⁴ Access Act, section 59 and section 65.1; Private Sector Act, section 12 and section 13.

¹⁵ Access Act, section 65.0.2; Private Sector Act, section 8.3.



Consent must be free

2.1. Free character

Consent **must** be **free**, that is, it must involve real choice and control, and it must be given without coercion or pressure. The person concerned **must** therefore be able to exercise its will without being unduly influenced or suffering disproportionate harm.

2.2. Fair mechanisms

It **must** be as easy to provide one's consent as it is to decline providing it. These options **should** be presented fairly. Consent mechanisms which do not guarantee the fairness of options, or that otherwise influence the user's choice, do not elicit truly free consent and thus could ultimately lead to invalid consent. For example:

- a. Emphasizing acceptance rather than refusal, regardless of the manner in which it is executed: visual highlighting (colors, font size, etc.), efforts the user must deploy in terms of clicks or web browsing, intentionally ambiguous wording, misleading text, etc.;
- b. Seeking consent repeatedly when it has already been refused may be contrary to its free character. Consent **should** usually only be requested once for the same purpose, unless a substantial change in context justifies it.

See examples [2-a](#) and [2-b](#).

2.3. Consent as a condition

In principle, consent is not free if it is an indispensable component of the conditions of use of a service, provision of a good, or access to employment. Organizations **must** therefore allow individuals to refuse **secondary purposes without impacting on the original agreement**.

However, in certain cases, the use of disclosure of personal information for which consent is required is necessary for the provision of a product or service, or for access to employment. In such cases, it is linked to the organization's **primary purpose**. Where the organization complies with its transparency obligation, consent is presumed for use and disclosure for primary purposes if the individual provides his or her personal information¹⁶ (see [section B.6](#)). If the individual does not provide this information, the organization cannot provide the service or good, or access to employment, and is therefore within its rights to refuse¹⁷. An organization must ensure that the use or disclosure is necessary in the circumstances.

See examples [2-c](#) and [2-d](#).

2.4. Change of purpose

Where an organization pursues a new purpose that requires consent of persons concerned by personal information (see [section 4.5](#)), that consent shall not be considered free if the organization indicates that it will cease providing services to those who refuse to provide their consent for the new purpose. In such a case, the organization **should** still be able to demonstrate that this new purpose is necessary for the continuation of the service (see [section B.3](#) and [section 2.3](#)).

¹⁶ Access Act, section 65.0.2; Private Sector Act, section 8.3.

¹⁷ Private Sector Act, section 9.

2.5. Situations of imbalance

Situations in which there is an imbalance of power between an organization and a person concerned may threaten the free nature of consent. This is particularly the case in employer-employee relations, where the CAI recognizes that the laws do not provide a clear solution in such circumstances. An organization **should** adopt measures appropriate to its context to mitigate this problem if it is intending to rely on consent. It may, for example, offer other options for how a purpose may be achieved so that a person still has control over their information. In all cases, an organization **should** pay particular attention to transparency so that any persons concerned are as informed as can be, and so that their other rights (complaint, access, rectification, etc.) are preserved (see [section B.2](#)).

See examples [2-e](#) and [2-f](#).



2.6. Withdrawal of consent

Consent may be withdrawn at any time by the person concerned¹⁸. An organization **should** provide a simple and accessible mechanism for withdrawing consent and **should** notify persons concerned. The fact that a person must make disproportionate efforts to exercise their right to withdraw their consent may have consequences for the free nature of such consent.

See examples [2-g](#) and [2-h](#).



¹⁸ Access Act, section 65; Private Sector Act, section 8.



Consent must be informed

3.1. Informed character

Consent **must be informed**, that is, precise and based on appropriate knowledge. The person concerned **must** know and understand what they are consenting to and what it entails. If the organization does not provide the necessary information, the control exercised by the person concerned is illusory and the consent is invalid.

3.2. Capacity of the person concerned

In order to be informed, consent **must** first be given by a person who is able to bind themselves at the moment when they manifest their consent¹⁹. For example, consent given by an incapacitated person or a person under the age of 14²⁰ is not valid. In such circumstances, consent may, however, be provided by a representative, such as the holder of parental authority or another representative.

3.3. Parallels between transparency at the time of collection and informed consent

An analogy can be drawn between the information an organization **must** provide to persons concerned at the time of collection²¹ (see [section B.3](#)) and the information it **should** provide for consent to be informed. Indeed, the law stipulates that individuals who provide their information after having received the information required by law at the time of collection consent to the use and disclosure necessary for the primary purposes stated²² (see [section B.6](#)). The legislator therefore believes that this information allows the person concerned to make an informed decision regarding his or her personal information.

Consequently, to ensure that consent is informed, an organization **should** provide the information presented below, which is inspired by section 65 Access Act and section 8 of the Private Sector Act, with the necessary adjustments, depending on the context. **Sections 3.4 and 3.5 are not guidelines for the application of these sections in a collection context.**

3.4. Information to be provided

In order for the person concerned to make an informed decision, an organization should generally provide the following information when obtaining consent:

- a. **Who?** The organization on whose behalf consent is sought;
- b. **Why?** The purpose of the consent request;
- c. **What?** Relevant information, or at least classes of information; as a reminder if a certain amount of time has elapsed since the information was collected;
- d. **With whom?** Where applicable, the names or classes of third parties outside the organization from whom or for whom the organization will collect the information;
- e. **How?** Means of using or disclosing the information (e.g. mail communication; use of a fully automated decision);

¹⁹ *Civil Code of Quebec*, section 1398.

²⁰ Access Act, section 53.1 and section 64.1; Private Sector Act, section 4.1 and section 14.

²¹ Access Act, section 65 and section 65.0.1; Private Sector Act, section 8 and section 8.1.

²² Access Act, section 65.0.2; Private Sector Act, section 8.3.

- f. **To whom?** Where applicable, the names of third parties or class of third parties external to the organization to whom the organization will disclose the information;
- g. **Outside Quebec?** Where applicable, possibility of the information being disclosed outside Quebec;
- h. What rights? Right to withdraw consent, right of access and right of rectification, with details on how to exercise them.
- i. **Accessible to whom?** Categories of individuals within the organization who will have access to the information in order to achieve the intended purpose;
- j. **Until when?** Period of validity of the consent (see [section 7](#));
- k. **Who to contact in case of need?** Contact information of the Privacy Officer, from whom individuals can obtain further information or exercise their rights.

See examples [3-a](#) and [3-b](#).



3.5. Accessibility of information – levels

A lot of information needs to be provided. An organization **should** structure the information in several levels to make it easier for those concerned to understand. To establish the number of levels and their content, it **should** then take into account various elements: the context of its activities, the expectations of the persons concerned, the sensitivity of the information in question, any changes that have occurred since the information was collected that may affect its processing, whether the information should be accessible on request, etc.

For example, it is possible to prioritize information into two levels:

- a. The **first level** (e.g. the consent request) may include:
 - i. The **purpose** (why);
 - ii. The **information or categories of information concerned** (what);
 - iii. **Third parties**, if any (to whom/from whom).
- b. The **second level** could include other information. This second level could consist, among other things, of:
 - i. A privacy policy, including that required by law when a technological means is used to collect information²³;
 - ii. An annex to a form;
 - iii. A question mark icon or “Learn More” button next to the consent request.
 - iv. For verbal modalities, an indication that further information is available on request.

See examples [3-c](#) and [3-d](#).



3.6. Precision and clarity of terms used

The elements presented above should allow for specific consent (see [section 4](#)) through the provision of simple and clear terms (see [section 6](#)). An organization **must** therefore avoid vague, imprecise or overly complex language, as well as long or legal jargon-rich texts. Such factors make it difficult for people to fully understand what they are consenting to.



23 Access Act, section 63.4; Private Sector Act, section 8.2.

3.7. Separate information for each purpose

When a request for consent to secondary use or disclosure is made at the time of collection, an organization **must** ensure that it provides:

- All information required to meet its transparency obligations regarding collection, including the primary purposes for which it collects information²⁴;
- Information relating to all other purposes for which it requests consent. However, in such as case, it **must** do so separately from the information provided for primary purposes (see [section 5](#) and [section 8](#) for written requests). As a result, a link is established between the informed consent of the person concerned, and the amount of information provided simultaneously to them: presenting the information separately, especially as it concerns consent, reduces potential for confusion.



See example [3-e](#)



3.8. Availability of information

Since consent that is free may be withdrawn, an organization **should** once again provide the relevant information to the person concerned, on request. This way, the person can reassess his or her decision after giving consent, if necessary (see [section 2.6](#)). An organization **could** deploy means to make such information readily available by default for future reference, for example on a website.



3.9. Duty of assistance

An organization **must** assist individuals seeking assistance in order to understand the scope of the consent being sought. The organization is responsible for developing mechanisms to this end, according to the context of its activities. For instance, it **could** provide a toll-free telephone number or live online chat service to contact a manager, or set up a dedicated e-mail address to receive questions.

See example [3-f](#)



²⁴ Access Act, section 65 and section 65.0.1; Private Sector Act, section 8 and section 8.1.



Consent must be specific

4.1. Specific character

Consent must be **given for a specific purpose**, i.e., for a specific and limited purpose.

4.2. Link to informed character

This criterion is closely linked with the criteria of informed consent: a person can only consent if they are able to understand exactly what is being asked of them.



4.3. Specificity of terms

An organization **must** ensure that the terms it uses to describe the purposes for which consent is sought are as specific as possible. Vague, broad, or imprecise terms threaten the specificity of consent, and thus its validity (see [section 6](#)).



See examples [4-a](#) and [4-b](#).



4.4. Restriction of use

In order to respect the specific wishes of persons concerned, an organization **must** rely on consent only such consent authorizes. Consent expressed by a person is restrictive: it applies only to the purposes that the individual was informed of, and only applies to third parties that were specified.

See example [4-c](#).



4.5. New purpose, new consent

Where an organization wishes to use or disclose personal information for purposes other than those which individuals already consented to, the organization **must** obtain new consent from the individual, unless an exception is provided by law is applicable (see [section B.10ss.](#)).



Consent must be granular: it is required for each purpose targeted

5.1. Granular character

Consent **must** be **granular**, that is, **requested for each purpose described**. Granularity refers to the idea of a physical object whose parts can be distinguished from another.

5.2. Link to the free, clear and specific nature of consent

Granularity ensures that consent is truly free. Consent is not free if the person concerned must accept several purposes or third parties to whom the organization discloses his or her information at the same time, since the person's only choice is to refuse or accept in omnibus. In the same way, granularity ensures that the person concerned clearly expresses their will for each specific purpose.



5.3. Nuances of consent

To allow persons concerned to choose on a granular basis what they accept and reject, an organization **must** inform them of each purpose and, in the case of disclosure, list the third parties or categories of third parties who will receive the information. It **must** then allow individuals to express their consent or refusal separately, for each purpose and each third party or category of third parties concerned. It is not a question of duplicating all the elements relating to consent (e.g. multiplying the number of forms, giving the same information several times, etc.): the organization **must** only adapt its method of obtaining consent (see [section 1.4](#)) for the purposes of granularity.



See examples [5-a](#) and [5-b](#).



5.4. Granularity and implied consent

Since implied consent does not involve an active, positive act (see [section 1.3](#)), it is more difficult for this type of consent to be granular (see [section 1.7](#)). To avoid this problem, an organization that relies on implied consent should generally ensure that it concerns only one purpose.





A request for consent must be understandable: it must be presented in clear and simple terms

6.1. Understandable character

The request for consent **must** be comprehensible, i.e. presented in clear and simple terms, both in terms of information provided and specific inclusion of a statement of acceptance or refusal.

6.2. Link to the informed and specific nature of consent

This criterion serves to ensure that consent is informed, but also serves to prevent organizations from subsequently interpreting consent too broadly (specific nature of consent). Various elements may simplify and clarify the statements for the persons concerned, such as those presented in the following paragraphs²⁵.



6.3. Concision

Information presented should be concise, that is to say, it should be expressed with a minimal number of words, while still remaining clear. An organization **should** avoid unnecessary words, complex structures and too many periphrases. Text or sentences that are too long interfere with the understanding of the persons concerned.

See example [6-a](#)

6.4. Simple vocabulary

An organization **should** use simple terminology, that is, terms that are accessible to the persons concerned. It **should** prioritize common vocabulary items, without legal or organizational jargon.

See example [6-b](#)

6.5. Clarity of intent

An organization **should** use the most direct language possible to seek authorization from persons concerned, both in terms of presentation and formulation of the options available to them. The use of specific terms avoids confusion as to what acts are required of the person and preserves the legal significance of such acts. In the same way, terms expressing uncertainty or a hypothesis (e.g., verbs conjugated in the conditional form) **should** be avoided unless the organization can demonstrate why it is unavoidable to use them.

See example [6-c](#)

6.6. Adaptation to public

An organization **should** tailor information to the intended audience. To do so, an organization **should** consider the perspective and profile of persons concerned, as they may not have background information on their privacy rights and may not be familiar with the organization's activities. An organization **should** also tailor the terms used so that the information is reasonably understandable by the majority of those concerned.

See examples [6-d](#) and [6-e](#).

25 The plain-language principles of Web copywriting from Québec.ca's government design system might be a useful resource.



Consent must be temporary: it must be valid only for the duration for which it is necessary

7.1. Temporary nature of consent

Consent **must** be **temporary**, i.e., it must be **valid for a limited period of time**. It shall be valid only for the period which is necessary to achieve the purposes for which it was requested. Accordingly, it is no longer valid when such purposes are fulfilled.

7.2. Limitation of duration

The duration limit is associated with the intended purpose. This purpose is deemed achieved on the basis of one of the following two elements:

- a. **A time limit:** after a period of 30 days, one year, six years, etc.
- b. **An event:** when an event occurs (such as when a payment is completed, as soon as a student leaves university, as soon as a contract ends, etc.)

An organization **must** define in advance the length of time required to achieve the purpose. It **should** inform the persons concerned thereof (see [section 3.4](#)). The duration limit further contributes to making consent specific (see [section 4](#)).



See example [7-a](#)

7.3. Distinction between duration limit of consent and the retention period

The duration of the validity of consent is a different concept from the retention period. The expiry of the validity of a consent does not always coincide with the destruction of the information.

The duration for which an organization may retain information thus depends not only on the purposes for which it was collected, but also on the laws applicable in its context²⁶. For example, many public bodies must comply with the *Archives Act*²⁷, financial players have retention obligations under sector-specific laws, and professionals must keep their records in accordance with regulations specific to their field.

7.4. Transparency as to consent valid for a lengthy duration

When an organization requests consent for a long period of time, it **should** pay particular attention to transparency on an ongoing basis. It **could** remind persons concerned, at appropriate intervals, that the basis on which the organization uses or discloses the person's information is consent. It **could** refer to up-to-date information on this situation (see [section 3.8](#)) and should remind persons concerned that it is possible to withdraw consent at any time. The organization **could** also disseminate this information through easily accessible means (e.g., a website).



²⁶ Access Act, section 76; Private Sector Act, section 23.

²⁷ The CAI is not responsible for overseeing the application of this law.



A request for consent shall be separate: it shall be submitted separately if it is in writing

8.1. Distinct nature

If a request for consent is made in writing, it **must** be made **separately from the provision of any other information**. It **must** therefore be separate from the terms of use, privacy policies, requests to confirm the validity of information provided, commitments, signatures, etc. The request for consent **could** be featured in its own section or on its own interface (section of the form, overlay window in an application, etc.), and thus easily accessible to the persons concerned.

See examples [8-a](#) and [8-b](#).



8.2. Link to other validity criteria

The distinctiveness of the request for consent is interrelated with other the criteria required for valid consent, including:

- a. **Clear and free:** Consent is not clear if expressed by a gesture that can also attest to something else, such as the receipt of information or the validity of the information provided, since the intentions behind the gesture are inseparable (see [section 2.3](#)). Consent in this context is also not free, since it is difficult to express a refusal in these circumstances.
- b. **Informed:** Requests for consent presented separately from another help limit the amount of information provided concurrently, and thus facilitate the understanding of the person concerned.



See examples [8-a](#) and [8-b](#).



Examples

As mentioned in [section A.5](#), the following examples aim to illustrate the guidelines. They are fictitious but may be based on actual practices. Since they aim to highlight specific aspects of the text - for example, a single validity criterion – they present deliberately simplified situations. In practice, each context requires its own specific analysis.

These examples are therefore tools. When a potentially non-compliant situation is described, the CAI suggests a course of action, but this should not be regarded as the only possible solution.

Although the examples are generally associated with one sector, public or private, they may inspire organizations in the other.

Each example contains one or more clickable links to the relevant paragraph(s) in the guidelines.

D. Examples related to the introduction

Example	Section concerned
<div data-bbox="94 1073 188 1167" data-label="Image"> </div> <p data-bbox="94 1178 261 1205">Private sector</p> <p data-bbox="305 989 472 1016">Example B-a</p> <p data-bbox="305 1041 1312 1289">A dating application allows users to determine a larger or smaller area around their position to filter potential partners based on their proximity. Upon registration, the application presents various information required by law when collecting information. A notice informs users that it includes a localization feature that is deactivated by default. In order to access this feature, users must enable geolocation on their mobile device and allow the application to access it. The application informs them of the means available to do so.</p>	Section B.4
<div data-bbox="94 1461 188 1556" data-label="Image"> </div> <p data-bbox="94 1566 261 1593">Private sector</p> <p data-bbox="305 1331 472 1358">Example B-b</p> <p data-bbox="305 1383 1312 1673">A magazine’s website provides recommendations personalized articles based on readers’ interests, inferred by an algorithm that employs artificial intelligence. The information used for inference (pages visited, clicks, browser language, time spent on each page, etc.) is collected using cookies stored on the reader’s device. Since this technology allows profiling, the magazine displays a superimposed window over the content during the reader’s first visit to the site and provides the persons concerned with the information required by the law. It then tells them how to <u>activate</u> the installation of cookies.</p>	Section B.4

Example B-c

At its general assembly, a condominium association adopts a unanimous resolution in favor of the installation of surveillance cameras as a preventive measure against vandalism. The cameras are positioned at an angle that allows the entry door of each unit to be filmed.

Despite the agreement of the co-owners, which establishes their consent, capturing images throughout the building may not be proportional to the security objective pursued. The invasion of privacy of co-owners and their guests is significant: the angle of the cameras means that everyone's comings and goings can be filmed. In these circumstances, the installation of surveillance cameras by the condominium association may not meet the test of necessity. **Consent would not be sufficient to comply with the law. To ensure compliance, the condominium association could reassess the necessity of the video surveillance, for example, using a privacy impact assessment. It could consider modifying the camera angles to capture only the main entrance and exit doors of the building, so as to limit the invasion of privacy.**

[Section B.8](#)



Private sector

Example C-a

An organization has a policy and procedures related to the consent of customers to the disclosure of their personal information. **In order to document the process of obtaining consent, while collecting only the information required for this purpose, the organization stipulates that any verbal consent obtained over the telephone must be noted in the file of the person concerned. The agent collecting consent must also note the name, date and time of the call.**

[Section C.2](#)

[Section C.3](#)



All sectors

In recent years, the organization has also updated its telephone call scripts on three occasions. Each time, it has kept a copy of the previous versions. **If necessary, this would make it easier to demonstrate that consent obtained under a previous version of the scripts was well informed.**

Example C-b

A Crown corporation providing digital services frequently updates its online consent forms. Each time, it saves the previous version in its archives. Each version of the form recorded is accompanied by an indication of the period it represents. **This practice allows the Crown corporation to keep track of the documentation which allows them to assess the validity of consent obtained at an earlier time. Archived forms could thus be used in the event of an inspection, for example.**

[Section C.3](#)



Public sector

E. Examples related to clear consent

Example

Section
concerned

Example 1-a

A public agency’s employee provides services to persons with motor difficulties, the majority of whom cannot write or use touch screens. To validate eligibility for financial assistance, the employee must communicate information from the files of such individuals to a ministry. The governance rules of the agency exclude the use of exceptions to consent when it is, in practice, easy to obtain consent (e.g. where a small number of individuals are involved). The employee thus relies on the express consent of the persons concerned for the communication of information. **To ensure that the specific characteristics of the customers to whom the services are provided are considered, the employee requests consent orally during the next meeting with the persons concerned. The date, time and details of consent are recorded in the file.**

[1.4](#)



Public sector

Example 1-b

A manufacturer markets an educational connected toy for children aged 5 to 8 years. The toy can record the child’s first name, and measures the child’s weekly progress in terms of their responses to letters and numbers (correct or incorrect answer, response time, etc.). The results are available on a secure web portal for parents. The manufacturer must obtain parental consent to collect this information from the children. During its initial configuration, the toy provides audio instructions to the parents. **To consent to this collection from their child, parents are asked to log on to the web portal and check an acceptance or refusal box. This mechanism allows the manufacturer to obtain the parents’ express consent.**

[1.4](#)



Private sector



Public sector

Example 1-c

In order to respond more efficiently to citizens' requests, a government agency wishes to design a system that uses artificial intelligence to prioritize files (AI System). It plans to develop the AI System using data on service usage on from the last three years. On the basis of a privacy impact assessment that was conducted, the agency's Committee on Access to Information and the Protection of Personal Information believes that express consent is required to use the information for this new purpose. Nevertheless, the agency decided to send an email out to the concerned citizens informing them of this new use, stating that they may contact the agency's Privacy Officer to withdraw their consent for this new usage. **This deduction of consent, based on the silence or inactivity of persons who will not contact the organization to withdraw it, does not offer the possibility of a positive gesture of acceptance. Therefore, consent is implicit rather than express. To comply with its committee's orientations, the organization could, for example, have asked citizens to give their consent via a personalized Web link associated with their file.**

[1.4](#)

Public sector

Example 1-d

An organization that provides benefits to persons with disabilities holds sensitive information about such individuals' health and financial situation. As part of the organization of a provincial conference on the integration of disabled people, the organization wishes to produce case studies of its beneficiaries in order to present them to the participants. As part of the organization of a provincial conference on the integration of disabled people, the organization wishes to produce case studies of its recipients in order to present them to the participants. However, at the time when the information was collected to pay the benefits, the organization made no mention of this secondary use. **In order to use the personal information of the beneficiaries in question, the organization must obtain their express consent, given that the information is sensitive. To ensure that this consent is expressed unequivocally, the organization could develop a self-supporting form and send it to the beneficiaries for signature.**

[1.6](#)

Private sector

Example 1-e

A massage therapy clinic organizes a series of conferences on health and wellness in collaboration with other health care providers. The owner of the clinic wants to send personalized invitations to her clients. She plans to use patients' health data and medical history in order to target certain customers and invite them to conferences. **However, she cannot use sensitive information for this secondary purpose without express consent. If obtaining express consent from each customer is too difficult, the owner might instead decide to announce conferences in the clinic's newsletter, which is already sent to customers who have agreed to receive news about events.**

[1.6](#)



Private sector

Example 1-f

After a series of break and enter attempts, an explosives manufacturer wishes to tighten access control to its storage site housing reactive materials in order to limit access to authorized personnel only. They plan to purchase a biometric system allowing for hand-shape recognition. Based on a privacy impact assessment that takes into account the context of its operations, the company concludes that the use of this technology meets the necessity criteria in this situation. Since the system relies on biometric characteristics, **the company recognizes that it needs express consent and develops a consent form²⁸. Employees who wish to do so can sign the consent form and those who refuse can opt for an electronic access card system.**

[1.6](#)

Public sector

Example 1-g

An elementary school offers an introduction to photography course/workshop an extracurricular activity for grade 5 and 6 students. Parents validate their child's registration in the program through paying the associated fees. In November, students attend a portrait workshop and take photos of each other. Particularly proud of the results, the teacher in charge of the activity selects five photos of children and sends them to the school's management for publication on the school's "parents portal", in aims of highlighting the activities offered by the school and the children's progress. Both the teacher and the school's management assessed that parents would be in favor of this dissemination, since they had been informed of the portrait workshop and since the "parents portal" was secure and accessible only to parents of pupils.

This implied consent is unlikely to be valid in these circumstances. Parents probably do not reasonably expect portraits of their child to be available digitally to several hundred parents without express consent. In the context of widespread dissemination, photographs of children could be considered sensitive, and the risks of serious harm arising from their dissemination should be adequately assessed. For these reasons, the school should have relied on express consent. This would have enabled the school to send an electronic consent form to the parents concerned via the secure portal.

[1.6](#)

²⁸ Section 44 of the *Act respecting the legal framework for information technology* requires express consent to verify or confirm a person's identity by means of a process that allows biometric characteristics or measurements to be recorded.

Example 1-h

An appliance rental company receives an application to rent a refrigerator for a period of 48 months. The automatic acknowledgement of receipt e-mail sent to the applicant indicates that, after a credit inquiry conducted by a personal information officer (whose is mentioned by name in the email), the company will provide funding at a favorable rate for the 48-month period. In a separate section of the email, it states that if no contrary indication on the part of the applicant is received, the company will provide the officer with the necessary identity information after three days. Since the applicant did not respond, the company proceeds with the credit inquiry for financing, affecting the applicant's credit rating. The applicant complains to the company, indicating that they intended to pay for the lease without obtaining financing. **In this situation, the company was not entitled to rely on implied consent for the credit inquiry request: doing so would go against the reasonable expectations of the applicant, who had not requested financing, and also caused significant harm to the applicant by lowering his credit rating. The company should have opted for a method of obtaining express consent to request a credit check.**

[1.6](#)

Private sector

F. Examples related to free consent**Example****Section
concerned****Example 2-a**

A municipality offers 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 email address, which serves as an identifier, and a postal code to initialize the default area displayed in the maps available in the application. They can then access all services through the app itself and see how their reports are being processed.

The app also allows users to use their email address to receive updates on road work in their area. The municipality displays a superimposed window for obtaining such consent. The application also allows them to use their e-mail address to receive updates on the status of roadworks in their area. The municipality provides an overlay window to collect this consent. **Users are presented with two buttons, “I accept” and “I refuse”. This makes it as easy for them to give their consent as it is for them not to. In addition, these buttons are exactly the same height, color and font size. By ensuring fairness in the visual presentation of choices, the municipality further promotes the free nature of the consent obtained.**

[2.2](#)

Public sector



Private sector

Example 2-b

A clothing store website allows customers to create an account to facilitate online shopping. Each time they log on, an alert is displayed, offering them the chance to receive the store's weekly newsletter, which includes discounts that may be of interest to them. It is as easy to accept as it is to refuse this secondary use of the email address. However, in the event of a refusal, the window will appear each time the client makes subsequent connections. **These repeated, closely spaced requests for consent, without regard to the wishes already expressed by the customer, may compromise its free character. To avoid this problem, the store could ensure that a reasonable time interval (e.g. a few months) separates these requests.**

[2.2](#)

Public sector

Example 2-c

In its application form for prospective students, a public university explains that personal information collected will be used to assess the application and to communicate student status to the appropriate department, in the case of international students (primary purposes).

However, in a separate section entitled "Foundation", the university seeks consent for a secondary purpose:

"I agree that my name, telephone number, email address, date of admission and field of study be communicated to the University Foundation for philanthropic purposes. This consent is valid for up to 5 years after my graduation.

Yes No"

The university adequately presents this secondary purpose, which is not essential to admission. The university gives the applicant full freedom to refuse this communication to the foundation, without affecting the rest of their application. In doing so, the university ensures that the consent is free.

[2.3](#)

Private sector

Example 2-d

When selling a new car, a dealer uses a form to obtain the information necessary to provide financing to their customers. In the consent section, the dealer adds the following: "By signing this agreement, I agree that my email address and my name will be used to send me promotional offers for the duration of the financing." When questioned by a confused client, the business owner indicates that this condition is mandatory in order to receive financing. **The approach used here does not allow a person concerned to reject the secondary purpose, that is, the sending of promotional offers. The dealer therefore has not obtained valid consent, as it is not free. He should review this practice to offer customers a real choice to refuse receiving promotional offers.**

[2.3](#)

Example 2-e



Public sector

An inspection team from a surveillance agency works at a food company. On this occasion, the team's superior photographs his employees at work in order to include the image in the inspection report. A newspaper is interested in the inspection and requests that the photo be used in its article. The team manager considers sending an e-mail to the employees concerned to ask them if they agree to have the photo sent to the newspaper and used in its article in the paper edition of the newspaper the following day. **Given the power dynamic between the manager and their employees, the manager must ensure that the wording of the request for consent does not give rise to any negative consequences for a possible refusal to communicate. If employees feel compelled to consent to this communication, consent cannot be considered free. It must therefore be as neutral as possible in its request. It would also be a good idea to invite each employee to reply separately, to avoid any pressure from the group.**

[2.5](#)

Example 2-f



Private sector

A private laboratory decides to adopt a biometric access control system to restrict access to a room containing a machine that uses highly radioactive material. The standards of the nuclear safety agencies require particularly strong security in order to limit the risk of theft or sabotage of this type of material. In the consent form provided to employees, the company explains the purpose of the system and indicates that employees who do not wish to have their biometric information collected²⁹ will be able to authenticate themselves in other means. They will be required to present an access card and then validate their identity with a security guard. Both biometric access and traditional access cards allow persons concerned to retain control. **In these circumstances, the laboratory has made reasonable efforts to preserve the freedom of consent, despite the employment context: employees can refuse collection and opt for a different authentication solution.**

[2.5](#)

Example 2-g



Public sector

A university research laboratory team is conducting a study on voice perception. To build its material, the lab recruits participants to be recorded as they recite a text. They sign a consent form that includes all required information and allows researchers to reuse the voice of participants in future studies on other specific subjects for five years. Participants who, at some point, no longer wish to have their voice used by the lab may withdraw their consent by sending a simple email to the laboratory's common address. **This withdrawal mechanism is simple and accessible. It does not constitute a barrier to obtaining free consent.**

[2.6](#)

²⁹ Section 44 of the *Act respecting the legal framework for information technology* requires express consent to verify or confirm a person's identity by means of a process that captures biometric characteristics or measurements.

Example 2-h



Private sector

A music distribution company provides an application that allows users to access the albums they have purchased. A pop-up window appears the first time they log in allows them to activate custom recommendations for discovering music. An algorithm then profiles them based on the songs they are listening to, the duration of their listening and the time of day during which they are listening. A user decides to withdraw his consent to the use of this information for the purposes of personalized recommendations. The user must make eight clicks in the application’s various setup screens before finding the option to disable the feature. **While it takes only one click to consent to personalized recommendations, it takes many more to withdraw consent. In this context, these efforts are disproportionate and undermine the free consent on which the undertaking relies. The number of clicks to consent or refuse should be equivalent.**

[2.6](#)

G. Examples related to informed consent

Example

**Section
concerned**

Example 3-a



Public sector

A Ministry’s employee requires that a person concerned sign a generic consent form before all fields have been completed. The text presented to the person concerned reads as follows, absent any information appearing on the blank lines:

“I authorize the Ministry to provide the following information: _____
to the following persons: _____ for the following purposes:
_____.”

[3.4](#)

This approach does not allow for informed consent. When no information about what is being consented to is provided, the person concerned cannot understand the scope their consent. At the moment it is being sought, consent must be capable of being given with full knowledge of the facts. The Ministry could instruct employees to always fill in the blank lines before the persons concerned sign the forms.

Example 3-b

Two online purchasing platforms obtain the consent of buyers to share their contact information with other businesses so that they can send them promotional offers. They use different texts:



Private sector

Platform A: “I agree that [the Company] will share my contact information with partners.”

3.4

Platform B: “I authorize [the Company] to send my name and email address to its affiliates in the field of e-commerce for them to send me promotional offers.”

Platform B’s more comprehensive text is more likely to lead to informed consent Platform A’s text is, which does not disclose the purpose of the communication and does not give any indication as to the identity of its partners.

Example 3-c

A centre de services scolaire (CSS) wishes to fill a position that entails working with vulnerable persons. It is necessary in this context, the CSS needs to obtain, for each candidate, a “Police Certificate” from law enforcement attesting to candidate’s absence of a criminal record. The CSS requires the consent of the candidates to this effect. The hiring form contains a dedicated section for the consent to the disclosure of information to law enforcement, and for the disclosure of the “Police Certificate” by law enforcement to the CSS.



Public sector

To ensure that such consent is informed, the CSS includes all essential information in the consent request:

3.5

“CSS X [**who?**] needs your consent to share your identification information [**what?**] with Police Service Y [**with whom?**] in order to conduct a background check that attests that you can work with vulnerable persons [**why?**]. This consent also covers the provision of the “Police Certificate” by Police Service Y to CSS X [**what?**]. Additional information is available in Annex A.

I accept / I refuse”

Appendix A provides, at a second level, the additional information (rights, period of validity of consent, contact details for the Privacy Officer, etc.). CSS’s practice avoids overloading the consent application.



Private sector

Example 3-d

An accounting firm uses some of its clients' personal information for secondary purposes with their consent, which is obtained through the electronic portal available on the firm's website (collection by technological means). When consent is requested, the accounting firm states the purpose of the request for consent and specifies the categories of information which the request for consent relates to (identification information, financial information, etc.). The firm also clarifies that the consent is valid for the duration of the next fiscal year. It also includes a link to its privacy policy. By clicking on this link, a client views a superimposed window displaying a simple policy providing additional information (technical means employed in order process the information, explanations on the right to withdraw consent, etc.). **By displaying this information in a "second level," i.e. in an easily accessible privacy policy, the accounting firm ensures that an interested client can read the information before consenting, while avoiding overloading the content in the consent request. The consent obtained is therefore informed.**

[3.5](#)

Public sector

Example 3-e

In order to process reports of harassment, incivility or sexual misconduct, a university collects personal information from complainants through a digital form. The form contains an initial general text explaining the purpose of collection, an indication of the persons to whom the complaint must be sent to ensure compliance with applicable policy, and an indication of the mandatory nature of information required to process the complaint (surname and first name are exempt and can optionally be provided). The complainant's rights of access and rectification are also presented. At the end of the form, once the person reporting presses "Next," a separate page is displayed. The university requests consent to allow the complaints office to discuss the complaint with the department's management. Specific information concerning this consent is provided. **By providing the new information separately from the information needed to process the complaint, the university promotes informed consent to the disclosure.**

[3.7](#)

Private sector

Example 3-f

In order to access the services of an organization using a third-party authentication service online, a person must consent to the disclosure of certain identity information by that third party to the organization. In its privacy policy, which is easily accessible through a link on the consent page, **the organization indicates that it is possible to chat with an agent to obtain assistance in order to better understand the consent being sought. A toll-free number is also provided to allow customers to speak with an agent over the phone during business hours. These mechanisms are part of the organization's toolkit for providing assistance to those in need.**

[3.9](#)

H. Examples in relation to the specific character of consent

Example

**Section
concerned**

Example 4-a

A school obtains parental consent for so that a multidisciplinary team at the school may share information on a child with a health facility where the child has been receiving complementary services. The school asks parents to consent to “any information” being “possibly” shared with “any person who needs it”. **The use of such imprecise terms undermines the informed nature of parental consent, as well as its specificity. The school should specify:**

- **The specific purpose(s) (e.g., “to continuously adjust the child’s care plan to his or her needs”);**
- **Categories of information concerned (e.g. “information on the child’s psychomotor development”);**
- **Anticipated frequency of disclosure (e.g. “twice a month”);**
- **Anticipated categories of recipients (e.g., “professionals assigned to the child’s care at health facility X”).**

[4.3](#)



Public sector

Example 4-b

A union seeks the express consent of some of its members to use some personal information contained in active grievances to “improve its processes.” **This terminology is imprecise and undermines the specificity of consent, as it does not allow for a true understanding of the intended purpose. The purpose should be stated more clearly** (e.g. to “improve grievance staff training”, “training artificial intelligence to automate certain steps in grievance processes”, etc.).

[4.3](#)



Private sector

Example 4-c

An intermunicipal board receives a request from a company that wants to obtain the attendance record of one of the board’s employees, who is seeking to obtain a position. The Director of Human Resources (DHR) of the intermunicipal board contacts the employee in question to obtain their consent to release this file to the potential employer, which the employee agrees to. However, the DHR transmits the employee’s complete attendance record, which covers four years of service. **In doing so, the board does not respect the specificity of consent that was obtained, which related exclusively to the disclosure of the attendance record for the last year. The DRH should have carefully considered the period in question. The intermunicipal board could adjust its human resources personal information management procedures accordingly.**

[4.4](#)



Public sector

I. Examples related to the granular character of consent

Example

**Section
concerned**

Example 5-a

An organization that funds projects collects applications through a form. The organization wishes to seek the consent of the persons concerned for two purposes: (a) the communication of the candidate’s contact information to a broadcaster for the purposes of promoting the selected projects, and (b) the use of the person concerned’s email address for the purposes of sending a survey. The organization sets out a consent section, wherein these two requests for consent are made successively, and then includes a single box for the ‘I accept’ option, and a single box for the ‘I refuse’ option. **In doing so, the organization compromises the granular nature of consent, as the form requires a single authorization for two separate purposes. It should be possible for a person concerned to agree to the disclosure of their contact information for promotional purposes, while simultaneously refusing to consent to the use of their email address for survey purposes, or vice versa.**

5.3



Public sector

Example 5-b

A not-for-profit organization (NPO) holds a gala to present awards highlighting the work of certain practitioners in its field of activity. The organization collects email addresses from the candidates to inform them of their nominations and of the details of the ceremony. The organization also requests that candidates consent to three secondary purposes: (a) the use of their email address to contact them to assess their satisfaction after the event; (b) the use of their email address to send them the organization’s general newsletter; and (c) in order to allow the retention of email addresses by a company designated by the organization for official photography of the winners, so that they may offer discounts on other photography services. **In order to comply with the criteria of granularity of consent, the NPO has the three purposes in a table that include a corresponding “Yes” column and a “No” column for each purpose. Candidates may thus choose to accept or reject these three purposes separately:**

5.3



Private sector

“Consent. Do you consent that your email address will be:

- Used to reach you to gage your satisfaction after the event?

Yes No

- Used to send you our general newsletter?

Yes No

- Retained by the company designated for official photography of the winners to give you discounts on other services?

Yes No”

J. Examples related to the comprehensible character of consent

Example

**Section
concerned**

Example 6-a

In a consent form related to the provision of financial assistance, a Ministry uses text formulated in the following way:

“I authorize the Ministère **to forward to the rehabilitation service provider**, as soon as possible, **all information related to the holding of an account with a financial institution in order to proceed**, **if applicable, with the payment of my financial assistance.**”

6.3



Public sector

When the form is going through holistic review by the Ministry, it is changed to the following:

“I authorize the Ministry **to provide the rehabilitation center with the coordinates of my bank account to pay my financial assistance.**”

This improves the conciseness and clarity of the information without sacrificing critical information, which ensures that consent is comprehensible.

Example 6-b

A company requests consent using the following text:

“The Customer agrees to the Company’s automated analysis, including, but not limited to, historical transactional data for the purpose of determining a profile through machine learning; this profile will be used by the Company to issue, without however any formal commitment, and subject to applicable policies and procedures, personalized discount offers on the purchase price of certain products, provided that the Customer respects the terms of use.”

6.4



Private sector

This very legal style of text contains several words that are not common vocabulary, and includes several complex turns (long sentences, comma splices, etc.). The style of text may confuse the person concerned, thereby compromising their informed consent. The following text would be simpler and therefore more comprehensible:

“**Receive personalized offers** – I authorize the company to use my purchase history to determine my buyer profile using an artificial intelligence system. The company may choose to send me personalized discount offers tailored to my profile if I follow the terms of use of the application.”

Example 6-c

An organization reviews its procedures for obtaining consent at a time specified for review in its governance documents. The committee formed for the occasion notes that requests for consent seem generally to be made using vocabulary referring to knowledge rather than authorization: “I am aware that X-information will be used [...]” or “I understand that Y-information will be communicated to [...]”.

To clarify these requests, the committee modifies the text so that the verbs clearly evoke the concept of consent. “I consent to [...]”, “I authorize that [...]” or “I authorize the use of [...]” consent: “I consent to [...]”, “I agree that [...]” or “I authorize the use of [...]”.

[6.5](#)



All sectors

The Committee also notes that, on web interfaces, explicit options to accept or refuse consent are not situated on the interface (authorization or refusal): “Next” or “Ignore”, etc. **On the recommendation of its Committee, the organization shall standardize the options for presenting a choice between ‘Yes’ and ‘No’ as often as possible, or, if not, ‘I accept/I agree/I agree’ and ‘I refuse/I do not agree/I do not agree’.**

Through such changes, the organization is progressing towards clearer and simpler language and thus promoting informed and free consent.

Example 6-d

At the request of an Aboriginal nation that is increasing its language revitalization efforts, a team of researchers is conducting an in-depth linguistic study of elders in the nation, in partnership with an Aboriginal cultural institute. In order to allow the analysis of the data, the words of these elders are recorded in different situations (when going out into the territory, during family discussion, during a crafts session, etc.). In this context, participants are invited to tell a traditional story. The cultural institute wishes request that participants consent to the broadcasting of these recordings of stories on a section of its website dedicated to the language of the nation and the preservation of its intangible cultural heritage. To do so, the institute uses a form in French. However, some of the elders speak very little of this language.

In the particular context of this research, and in order to ensure that the request for consent is tailored to the audience, and that it is understandable to the audience, the cultural institute mandates a bilingual officer to obtain the oral consent of these participants and to answer their questions, if necessary.

[6.6](#)



Public sector

Example 6-e

A company offers a photo-sharing application to a very diverse population, including youth aged 14 to 17. In order to ensure that its consent procedures are clear to this audience, the company conducts comprehension tests with certain users and makes necessary changes. **By adapting the text to the level of literacy of teenagers, the company increases the likelihood that the texts will be understandable for the majority of persons concerned, regardless of their age.**

[6.6](#)



Private sector

K. Examples related to the temporary nature of consent

Example

Section
concerned



All sectors

Example 7-a

As part of its hiring process for professionals, an organization asks candidates to provide two references, for the purposes of assessing the quality of the candidate’s work in previous positions, and for obtaining information on the assessments in their file. The organization sets out an electronic form for providing references.

[7.2](#)

Wishing to be transparent about the duration of the validity of consent, the organization specifies to candidates that it is valid only until a decision on the application is made. This consent is therefore limited in duration by an event.

L. Examples related to the distinct nature of consent

Example

Section
concerned



Private sector

Example 8-a

At the end of a change of status form for a professional body, the persons concerned must sign the following four statements:

- “1. I acknowledge having read the package leaflet [...].
2. I declare that the information provided is complete and accurate [...]
3. I agree that the order will disclose my information to the survey firm ABC [...]
4. I undertake to provide notice to the order when [...].

Signature : _____”

The request for consent (third statement) is not presented separately from other information, as it is one among three other statements that are not requests for consent. The clear and free nature of consent is also compromised by this situation. To correct it, the professional order could move the consent request to the beginning of the section, add “Yes” / “No” boxes and indicate that the signature applies only to the other three statements:

[8.1](#)

[8.2](#)

“Consent. I agree that the order will disclose my information to the survey firm ABC [...]

Yes No

By signing this form:

I acknowledge that I have read the package leaflet...

I declare that the information provided is complete and accurate [...]

I undertake to notify the order of [...].”

Signature : _____”

Example 8-b

When creating an account for an online game, players must tick a box indicating that they accept the terms of use, which can be accessed via a hyperlink. That being said, no reference to consent is included in the form. By clicking on the link, a player discovers that the terms of use contain, among other things, the publisher's privacy policy. The text mentions that by accepting the terms of use, the player consents that their friends list, device metadata, interactions with the game (clicks, hours, etc.), and conversations on the public server may be used for the purposes of targeted advertising, improving game experience and preventing cheating, among other purposes. By accepting the terms of use, the player also consents to their score being broadcasted on a public platform, accompanied by their pseudonym and the game history, in order to stimulate competition in the game.

[8.1](#)

[8.2](#)



Private sector

On the issue of consent particularly, the fact that this information is incorporated into a privacy policy that is itself incorporated within the terms of use that relate to a variety of other subjects compromises the distinctiveness of consent. Moreover, this situation threatens the clear character of consent (act indicating consent that cannot be separated from the act indicating acceptance of the terms of use), its free character (impossible to refuse or accept granularly) and its informed character (information difficult to access).

Calgary

Centennial Place, East Tower
520 3rd Ave S W, Suite 1900
Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal

1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa

World Exchange Plaza
100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400
Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com

Canada's Law Firm

Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.