Notice of Consultation

May 16, 2023

(2023-1)Guidelines on the Criteria for Valid Consent

Background and Objective

The *Commission d'accès à l'information* (CAI) oversees the application of Quebec's main privacy laws, namely the Act Respecting Access and the Private Sector Act (see updated administrative versions on the CAI's website). The CAI has been tasked with developing guidelines to facilitate the application of these laws. Given that a majority of the provisions of Law 25 (which amended the above referenced Acts) will be coming into effect shortly, the CAI has prepared some initial guidance on criteria required for valid consent. This initial guidance is **based on the text of the laws as they will be when provisions of Law 25 come into effect on September 22, 2023**.

The guidelines, provided at page 4 of this document (direct access here), are intended to help organizations and individuals subject to these laws in better understanding the relevant elements used to assess each of the statutory criterion that are required in order to obtain valid consent (Act Respecting Access, section 53.1; Private Sector Act, section 14). Examples are provided to illustrate the application of the guidelines. **The guidelines do not apply to the health sector.**[1]

Consultation

The CAI is holding a consultation for six weeks (ending **on June 25, 2023 at 11:55 p.m**.) in order to seek input on the text of the guidelines. In addition, the CAI wishes to explore the need for future guidelines, both regarding access to information and the protection of personal information.

The consultation includes two components, each directed at a different audience:

1. **The general public, and individuals and organizations subject to the laws:** a questionnaire is available on the Consultation Québec platform. It allows for a brief comment on the proposed text of the guidelines, in addition to suggestions for future guidelines.
2. **Preemptively targeted stakeholders**: 18 stakeholders have been identified by the CAI due their expertise, role in industry, or significance of their activities, and these stakeholders have agreed to submit a brief on the guidelines. The instructions will be sent to such stakeholders by email. The list of stakeholders is provided below on page 3. Such submissions will be made public following the end of the consultation period.

[1] The provisions of the *Act Respecting Health and Social Services*, which provide a framework for health information, are not within the scope of these guidelines, and constitute a separate consent framework

The CAI has opted to conduct a "joint" consultation (including both the general public and specific stakeholders) in part due to organizational constraints as to capacity to analyze comments. An objective of the CAI is to make the final version of the guidelines available within a reasonable time so that organizations may benefit from them as soon as possible.

Analysis of comments and feedback

The CAI is committed to analyzing the comments received in a serious and rigorous manner. It reserves the right to reject them in whole or in part if they are not relevant to the subject matter of the consultation. The CAI will prepare a feedback document presenting and addressing key comments received by September 2023.

The CAI's consultation is distinct from any of the other activities it carries out, including those which are judicial or supervisory. The comments received during the consultation will only serve to improve the guidelines. They cannot be used in the course of investigations carried out by the CAI, for example.

Influence of the consultative approach

The comments received will allow the text to be adjusted, where necessary. The examples, level of specificity, and format of the guidelines can be modified. The CAI's general guidance on provisions of legislation, on the other hand, is less likely to change; it will only be changed if comments reveal new elements [which are pertinent to] the analysis.

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

Limits of the consultation

The CAI:

- **Will not provide individualized answers** to questions about the legislation that are submitted to it during the consultation;
- **Will not process any briefs from persons who were not invited by the CAI to submit a brief**. It is possible, however, to become a targeted stakeholder in a future consultation. A section of the questionnaire allows organizations to request becoming a targeted stakeholder in the future.
    - The CAI invites you to contact stakeholders listed below (i.e. industry representatives) should you wish to share your views on the guidelines or if you would like to partner with them to produce a brief;
- **Does not undertake to follow up on any proposed topics for future guidelines**, but will take them into account in planning its future work.

Protection of personal information

Information about the collection of personal information by the CAI as part of the consultation is available on the Consultation Québec platform.

Questions about the consultation

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

BLG UNOFFICIAL TRANSLATION – 2023-06-08

List of stakeholders who will be submitting a brief

1. Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité
2. Ministère de la Santé et des Services sociaux
3. Barreau du Québec
4. Fédération des centres de services scolaires du Québec
5. Fonds de recherche du Québec
6. The Association of Access to Information and Privacy Professionals (AAPI)
7. Fasken Martineau DuMoulin, S.E.N.C.R.L.
8. Border Ladner Gervais, S.E.N.C.Rl.
9. Gowling WLG (Canada), LLP
10. Lavery de Billy, S.E.N.C.R.L.
11. Fédération des chambres de commerce du Québec
12. Conseil du patronat du Québec
13. Canadian Life and Health Insurance Association Inc. (CLHIA)
14. Canadian Bankers Association
15. Canadian Marketing Association
16. International observatory on the societal impacts of AI and digital technology
17. Option consommateurs
18. Ligue des droits et libertés

Commission d'accès à l'information du Québec

Guidelines 2023-1

Consent: validity criteria

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 of these guidelines is based on the law as it will be in force on September 22, 2023)

Version 0.1 - Document for consultation

(Note: these guidelines are not yet in force)

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

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 ARA).
2. **Objective.** The CAI is disseminating these guidelines in order to facilitate understanding of the criteria for valid consent that public and private organizations (hereinafter organizations [2]) must obtain from the individuals whose personal information is concerned. These criteria are set out in:

    a. The ARA, at section 53.1;

    b. The *Act respecting the protection of personal information in the private sector* (hereinafter the ARPPIPS), at section 14.

    Unless other provisions are explicitly mentioned in this document, the guidelines are exclusively aimed at the interpretation of these two provisions.

3. **Exclusions.** These guidelines do not address consent to the disclosure of *non-personal* information—such as technical or financial information, or trade secrets (ARA, sections 23, 24, 25 and 49).

    Nor are these guidelines intended to provide specific guidance on situations where consent is or is not required, except [to the extent provided as] general information in section 1.1. Section 1.1 focuses on the criteria which must be met when consent is required by law.

4. **Legal references.** These guidelines are based on the provisions of the ARA and the ARPPIPS as amended by the *Act to modernize legislative provisions as regards the protection of personal information* (2021, c. 25, or Law 25). The CAI has made administrative versions of the ARA and the ARPPIPS available, which incorporate the amendments from Act 25.

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 specific aspect of the text (for example, a single validity criterion). Most often, the examples are associated with a sector (public or private), though some apply to both. A single example sometimes accompanies a paragraph, when the CAI considers it to be a good illustration of its meaning for all sectors.

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* (CQLR, c. S-4.2), or general, such as the *Civil Code of Quebec* (CQLR, c. CCQ-91). In addition, obtaining valid consent does not negate the organizations' other legal obligations to protect personal information.

[2] The term 'organization' in these guidelines, includes covers even individual acts or undertakings by members of the organization.

1.1. Consent is at the heart of the principle of individual control over one's personal information

7. **Notion of consent.** By default, personal information is confidential. Persons concerned can exercise control over the use and flow of their information through their consent. Given that consent is linked to personal autonomy, consent in this context means that an individual consents to what happens to their information. Consent is an important concept within Quebec's privacy laws.

   In order to comply with the law and thus be valid, consent must meet certain criteria. These guidelines focus on how to comply with each criterion.

8. **General rule.** These guidelines are not intended to establish the exact circumstances in which consent is or is not required. That being said, applicable laws generally require organizations to obtain valid consent in the following situations (non-exhaustive list):

   a. To collect personal information from a minor under the age of 14 (ARA, section 64.1; ARPPIPS, section 4.1) - consent is then given by a parent or guardian;

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

   c. To use personal information for secondary purposes, i.e. for purposes other than those for which it was collected (primary purposes) (ARA, section 65.1; ARPPIPS, section 12);

   d. To disclose or divulge personal information to a third party (ARA, sections 53, 59 and 88; ARPPIPS, sections 13 and 40).

   In addition to allowing for the authorization of the person concerned to be provided to the organization, a request for consent also functions to ensure transparency. A request for consent forms part of the information that apprises an individual of what the organization intends to do with their personal information.

9. **Exceptions.** In some cases, the ARA and the ARPPIPS 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 are not applicable, since there is no requirement to obtain consent.

10. **Use of exceptions.** Under the principle of responsibility (ARA, section 52.2; ARPPIPS, section 3.1; see section 1.3), an organization must be able to demonstrate that an exception allows it to use or disclose personal information without consent. It must also demonstrate transparency [to that effect].

    An organization intending to avail itself of such consent exceptions should therefore clearly describe any actions taken absent consent in their privacy policy or any other similar document. As a result of such a disclosure, individuals are informed of what happens to their information whenever the organization collects, uses or discloses it, thus preserving their rights to access, rectification, and de-indexation, and their rights

to file a complaint with the organization or the CAI, etc. Indeed, to exercise these rights, one must be adequately informed.

11. **The optional nature of exceptions.** Most exceptions, however, are optional. Organizations are not obliged to rely on consent exceptions and can therefore opt to rely on consent instead, especially when obtaining consent poses no practical difficulties (small number of people involved, easy-to-reach people, non-urgent situation, etc.).

    Depending on the context, relying on consent may sometimes be more beneficial to the organization, for example to facilitate demonstrable compliance (see section 1.3). Importantly, consent can also be later withdrawn by an individual (see section 2.2), providing an additional means of control over one's own personal information, in addition to the rights mentioned above. This may be part of an organization's analysis of whether it opts to rely on exceptions to consent for some of its activities.

12. **Irreversibility.** If, for a specific purpose, an organization chooses to rely on consent rather than an applicable exception for the collection, use or disclosure of personal information, it must respect the choice of the individuals involved. Thus, an organization cannot, when an individual refuses to consent or withdraws their consent, instead choose to rely on for the same purposes. The contrary would render consent meaningless as a means of control that individuals have over their personal information.

13. **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.

14. **Deemed consent**. When a person concerned provides their personal information after having received the information required by law (ARA, section 65; ARPPIPS, section 8), they are presumed to consent to the use and disclosure of their personal information for the purposes that justify its collection and of which they were informed (ARA, section 65.0.2; ARPPIPS, section 8.3).

    This deemed consent implies that an organization is not required to assess whether the validity criteria have been satisfied. However, a person concerned may subsequently withdraw their consent.

15. **Consent and necessity.** At all stages of the lifecycle of personal information, including during collection, use, disclosure, retention and destruction, applicable laws the law impose a necessity threshold to ensure that the information is necessary for the purpose for which it is to be used. (e.g. ARA, sections 64, 65.1, 67; ARPPIPS, sections 5, 12, 18).

    Consent never allows the requirement of necessity to be waived. It cannot, therefore, be sufficient in and of itself to authorize actions linked to personal information.

[A priori non-compliant practice*]*

Example 15.1 - At its general meeting, an association of 16 co-owners adopts a unanimous resolution in favor of the installation of surveillance cameras capturing images in all corridors in the condo building, so as to ensure the security of the premises. There is no history of significant safety issues. The cameras purchased are positioned at an angle that allows the entry door of each unit to be filmed.

Despite the unanimous agreement of the co-owners, which establishes their consent, the fact of capturing images in all parts of the building is likely, with respect to co-owners and their guests, to be an invasion of privacy with an impact that is disproportional to the security objective pursued. Indeed, people have an expectation of privacy when they are in residential spaces, and the positioning of the cameras means that the whereabouts of co-owners, in addition to the people they associate with is recorded and documented. Moreover, the security problem is theoretical and remains to be proven, since there is no history of significant safety issues. **In these circumstances, the collection of videotapes by the condo association fails to meet the test of necessity, and consent is not sufficient to render it lawful.**

16. **Confidentiality incident.** Unauthorized access, use, or communication of personal information constitutes a confidentiality incident when provided for by law (ARA, section 63.9; ARPPIPS, section 3.6). If an organization detects a problem related to a failure in obtaining valid consent, it must comply with obligations applicable in the case of [confidentiality] incidents (such as keeping a log, notifying the CAI and affected individuals 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 salary. In the context of the organization of a holiday event, two employees in the Human Resources department use this banking information to send a request for an electronic fund transfer from those who have confirmed their attendance for the event and who must pay for their registration. **This secondary use is not permitted by any exception in law, and the concerned employees have not consented to it. This is therefore a confidentiality incident for the municipality. The municipality must log this incident in their confidentiality incident register, and must assess whether there is a risk of serious harm to persons concerned, in aims of determining whether to notify the CAI and the individuals in question.**

[A priori non-compliant practice*]*

Example 16.2 - A social network offers users the opportunity 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 social network offers third-party advertisers the opportunity to display advertisements to users who are already on their own customer lists. To do this, publishers upload their list to the social media tool, in an encrypted format, and the social network's algorithm verifies whether customers are users against this information. This information includes the phone number and email address in the user profile, which is compared against those contained on marketing lists. **In doing so, the social network uses this personal information without authorization, since it has not obtained the consent of the individuals concerned, and whereas no exception (consistent purposes, security reasons, application of a law, clear benefit of the person, etc.) applies. This is therefore a confidentiality incident.**

1.2. These guidelines represent the Commission's expectations

17. **Intended audience of the guidelines.** These guidelines are specifically intended for the following people within an organization:

    a. The person with the highest authority;

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

    c. Members of the Committee on Access To Information and the Protection of Personal Information;

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

    e. Personnel who collect consent(s) related to personal information.

18. **Intent of the CAI.** These guidelines represent the CAI's expectations of organizations when obtaining valid and meaningful consent. The additional clarifications provided by the CAI are intended to facilitate the application of the law.

19. **Legal force of the guidelines.** The legal force of the guidelines exceeds that of CAI guidance documents, but they do not have the force of law. Laws and regulations take precedence over the content of guidelines at all times.

20. **Application.** In carrying out its oversight functions, the CAI will take into account an organization's compliance with these guidelines. Organizations should make the necessary efforts to implement them. If they do not, they should be able to explain why.

21. **Evolution.** These guidelines may be amended at a later stage. Other guidelines, that are more [specifically] targeted at precise sectors of activity, for example, may serve to complement them.

1.3. Organizations must be able to demonstrate compliance

22. **Principle of responsibility.** Organizations are responsible for protecting the personal information in their custody (ARA Section 52.2; ARPPIPS Section 3.1). They must be able to demonstrate that they are complying with their legal obligations (principle of demonstrability), including both obtaining consent and ensuring the validity of consent.

23. **Methods of documenting consent.** In these guidelines, the CAI does not require a particular method of proving that consent has been obtained. Organizations need to develop methods that are appropriate to their context and activities. That being said, organizations must always minimize the collection of personal information: documenting evidence of consent should not require collecting more information than is necessary, depending on the context.

[A priori non-compliant practice*]*

Example 23.1 - To document that consent has been obtained for the disclosure of certain tax information to a third party, a ministry decides to retain audio recordings of entire telephone conversations, in which the individuals concerned give their consent to an officer. **This method risks not complying with the principle of minimization**, as it entails the collection of additional information (audio recording of the entire conversation) only to demonstrate compliance. Instead, the ministry could record the date and time of that consent was obtained, as well as the name of the staff member who received it, in a file.

[A priori non-compliant practice*]*

Example 23.2 - An insurance company wishes to document its obligation to obtain the consent of persons concerned by the disclosure of compensation information to a third party. Through its web form, the insurance company decides to record users' cursor movement patterns on the consent page, from the moment the page is]opened until the user ticks the "I consent" box, in order to demonstrate that the gesture comes from the user and it was considered. The organization also records the duration of the users' activities. **This method may not comply with the principle of minimization**, since it involves the collection of additional information (e.g., mouse movement patterns, duration of presence on page), and this, solely for the purposes of demonstrating compliance. Instead, the insurance company could record the ticked status of the box, as well as the date and time of the transaction, in the users' file.

24. **Documentation of the validity of the consent**. In addition to documenting the obtention of consent, organizations must be able to demonstrate its validity. Once again, it's 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 (information provided upfront, actions taken by the user which demonstrate their consent, and how such acts are differentiated from other actions taken, etc.) including, where applicable, keeping an history of such factual elements to demonstrate that the obligation to obtain valid consent was previously fulfilled.

[A priori compliant practice*]*

Example 24.1 - A Crown corporation providing digital services maintains an archive with screenshots of its online consent form. Each is accompanied by an indication of the period it represents. Each time a change is made to the form, the Crown corporation adds a new screenshot to its archive. **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, including in the context of an inspection.**

[A priori compliant practice]

Example 24.2 - A business operating a call center has policies and procedures related to the consent of customers to the disclosure of their personal information. In recent years, one of the procedures, which establishes a framework for service requests, has been updated three times. Each time the policy is updated, the company kept a copy of its previous versions. **If necessary, this will make it easier for the company to demonstrate, for example, that consent obtained under a previous version of the policy was well-informed.**

25. **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 themself (or their legal representative, where applicable). In doing so, the organization must aim for a reasonable degree of certainty that the individual giving consent has been authenticated, depending on the context of its activities. Where there is a legal representative, the organization should also verify the capacity of the consenting person (i.e. the holder of parental authority, the legatee, the representative, etc.), all the while still aiming for a reasonable degree of certainty. This may include validating certain personal information, but the organization should not retain or collect more information than is necessary.

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

2. CRITERIA FOR VALID CONSENT

27. Criteria. Valid consent is defined in sections 53.1 of the ARA and 14 of the ARPPIPS, 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."

28. Interrelationship between the criteria, and each criteria's individual importance. The criteria are interrelated. They are all important: if one is not satisfied, consent is invalid and has no 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.

2.1. Consent must be clear

29. The clarity characteristic of 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 or explicit, though it may be implicit in certain circumstances.

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

30. Prioritization of express consent. Consent is express (or explicit) 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.

An organization should prioritize express consent wherever possible.

31. Compulsory express consent. In some situations, express consent is required. For instance:

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

i. Sensitive information includes information that has a medical, biometric,[3] or otherwise intimate nature, or that entails a high level of reasonable expectation of privacy because of the context of its use or disclosure (ARA, section 59; ARPPIPS, section 12);

ii. Consent is not required for the use or disclosure of sensitive information for the primary purposes for which it is collected (ARA, section 65.0.2; ARPPIPS, section 8.3) or where exceptions to consent apply.

b. **Identification, localization and profiling:** Law requires that technologies which permit the identification, localization or profiling of an individual must be disabled by default; organizations must inform the persons concerned of the means to enable such functions (LAI, Article 65.0.1; LP, Article 8.1). This is equivalent to requiring express consent.

[A priori compliant practice*]*

Example 31.1 – An organization that provides benefits to persons with disabilities holds sensitive information about such individuals' health and financial situation. As part of an evaluation of one of its programs, the organization appoints an employee to study the effectiveness of this allowance, particularly from a client satisfaction perspective. At the time when information was collected in order to pay the benefits, the organization made no mention of a [secondary] usage for program evaluation purposes. In order to allow the employee to use the information of the 275 recipients of the allowance in question, the organization must obtain their express consent given that the information is sensitive. **In order to ensure that such consent is undisputed, the organization develops a self-supporting form and sends it to the beneficiaries for signature.**

[A priori compliant practice*]*

[3] In this regard, the Act to establish a legal framework for information technology (CQLR, c. C1.1, section 44) also re-quires the express consent of the person concerned before requiring the verification or confirmation of their identity to be carried out using biometric characteristics or measurements.

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

[A priori non-compliant practice*]*

Example 31.3 - A Crown corporation must produce statistics on diversity (sexual, ethnic, linguistic, etc.) among its employees in order to create an action plan against discrimination. Because the crown corporation does not have access to information on the sexual orientation of employees, the Human Resources team plans to use the information on the gender of the dependent spouse, contained in each employee's group insurance form, to calculate the proportion of employees with a same-sex spouse. **In these circumstances, the Human Resources team must ensure to obtain the express consent of the employees since the sex of their spouse is sensitive information: it is very likely to reveal sexual orientation, information protected by the *Quebec Charter of Rights and Freedoms*.**

[A priori non-compliant practice*]*

Example 31.4 - A massage therapy clinic organizes a series of 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 determine if treatments offered [at the conferences] are safe and relevant for individual clients and their respective situations. The clinic collected this information from clients when the clients first opened their file at the clinic. information was collected [by the clinic] when said clients opened their file. **This secondary use of sensitive (medical) information cannot be done without express consent.** Given that she did not request such prior consent, the clinic owner finally decides to announce the conferences in the clinic's newsletter, which is already sent to clients who have agreed to receive news about events.

[A priori compliant practice*]*

Example 31.5 - 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 its situation warrants 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 authorized personnel in order to allow for the collection and use of these characteristics for authentication purposes. Employees who wish to do so can sign the consent form and those who refuse can opt for an electronic access card system.**

32. **Method 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. Signing a document, ticking a box, or answering a question in the affirmative are ways to express consent (unequivocal active and positive gestures), but they are not the only options available.

[*A priori* compliant practice]

Example 32.1 – 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 agency 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 must therefore rely on the consent of the persons concerned prior to the disclosing of the information to the ministry. The employee requests such consent orally and records the date, time, and details of the consent obtained in file notes, in order to meet their obligation of demonstrability. **This mechanism allows for the obtention of clear (and, in this case express) consent that takes into account the particularities of the clientele to whom the services are provided.**

[A priori compliant practice]

Example 32.2 - A manufacturer markets an educational connected toy for children aged 5 to 8 years. The toy records 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. In order to provide consent for the collection of the progression information of their child, the toy asks parents to consent by simultaneously pressing three colored buttons on the front of the toy. **This mechanism allows for overt (in this case, explicit) consent, taking into account the device with which the parents interact.**

33. **Consent fatigue.** Depending on the context of its activities, an organization may need to take steps to mitigate consent fatigue. Indeed, every day, we are all asked to provide our consent in a multitude of contexts. In the digital world, providing consent 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 of the fact that they are providing their consent. This, particularly to ensure that they understand the information made available to them (informed consent criterion; see section 2.3).

[A priori compliant practice*]*

Example 33.1 – A government agency provides a mobile application that allows citizens to access all of its services. Because of the nature of its activities, citizens frequently interact with the app. Thus, the body often obtains consent. The app asks users to confirm their consent by answering a mathematical question (like 8 + 4). **It thus contributes to "disrupting the rhythm" and partly combats consent fatigue.**

[A priori compliant practice*]*

Example 33.2 - A bank's mobile application frequently solicits the consent of its customers for the disclosure of their personal information. When needed, it displays, on a random basis, a window superimposed on the application that includes simple and clear information and a consent button. The window opens for one minute, with a countdown, to give customers enough time to read the information and the request for consent. The buttons for accepting or refusing consent do not activate until the end of the specified period. **In doing so, the bank is "disrupting the rhythm" and partly combatting consent fatigue.**

34. Inadequate methods. Even taking into account consent fatigue, an organization cannot *presume* express consent: express consent must involve an active and positive (unequivocal) gesture. Accordingly, the following methods are not valid to obtain consent, as they do not allow the will of the persons concerned to be ascertained beyond doubt:

a. Use of pre-checked boxes;

b. Simply providing the possibility of subsequent refusal (*opt out*);

c. Deduction related to the person's silence or inactivity;

d. Deduction related to a separate act of the person.

Rather, 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 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. **Since the agency assumes consent and does not offer individuals the opportunity to make a positive gesture of acceptance, the agency has not obtained express consent.** Obtaining express consent could have been done, for example, by asking citizens to confirm their consent through a personalized web link connected with their file.

[A priori compliant practice*]*

Example 34.2 - 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 ARPPIPS (articles 8 and 8.1, in particular). The reader then has the option of accepting or refusing the installation of cookies for the purpose of [providing] personalized recommendations. To allow for this, two clearly identified buttons ("*Accept*" / "*Reject*"), that are presented on equal terms, appear at the bottom of the superimposed window. **This allows the magazine to obtain express consent.**

35. **Likelihood of the person concerned's intentions becoming confused.** For consent to be express, an organization must avoid displaying a request for consent in such a way where it is possible to confuse it with another action that an individual must take, such as the act of confirming that the conditions of use have been read. The organization must devise clear consent mechanisms for the persons concerned. This relates to the distinctiveness of consent (see section 2.8).

2.1.2. In certain situations, consent may be implicit

36. **Implied consent.** In some circumstances, consent may take an implicit (or tacit) form, including when the following additional criteria are met:

    a. If the implied consent does not pertain to sensitive information;

b. If the implied consent does not conflict with the reasonable expectations of individuals in the context;

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

In such cases, consent is not expressly stated. Rather, the organization deduces it due to the silence or inactivity of the person concerned or from a separate, unrelated action taken by the person concerned, that is not directly related to the consent.

In practice, however, organizations must remember that deemed consent (ARA, section 65.0.2; ARPPIPS, section 8.3; see paragraph 14) includes many situations in which implied consent might have otherwise been considered relevant. Cases where implied consent for secondary purposes is relevant are rare.

[A priori non-compliant practice*]*

Example 36.1 - 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.

[A priori non-compliant practice]

Example 36.2 - 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. When the applicant does 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.

[A priori non-compliant practice]

Example 36.3 - A municipal council agrees to address issues received over email from citizens during its meetings. Citizens must identify themselves by name and address. During council meetings, questions are read aloud by the Clerk, along with the names and addresses of those who submitted them. For transparency purposes, the meeting sessions are recorded and posted to the municipality's website for a period of five years. No audio masking is done prior to such posting, and so names and addresses are publicly disclosed. When questioned about this by a citizen, a representative of the municipal council explained that the council relies on implied consent, believing that those who send questions by email should reasonably expect their contact information to be released. However, no information to this effect is provided on the municipality's website. **In these circumstances, the disclosure may not meet the reasonable expectations of individuals and the implied consent may not be valid.**

[A priori non-compliant practice*]*

Example 36.4 - A tech start-up wants to develop artificial intelligence that can evaluate a person's feelings based on their facial expression. In order to collect data needed to train the algorithm, the company uses a data-harvesting Web-crawler that browses various websites, including social networks and personal blogs, to extract photographs of faces. The company would normally need to obtain consent from the person concerned in order to collect their personal information from third parties. However, the company considers that by posting their photos on the web, individuals have implicitly consented to the use of their photos for other purposes, including training an algorithm. **This collection may run counter to the reasonable expectations of individuals who share these photos knowing that other humans they know will view them, but who do not necessarily know that they will be used to train artificial intelligence.** Moreover, it is near impossible to inform the persons concerned of this practice, which causes a problem of transparency.

37. **Clear consent in all cases.** When choosing to rely on implied consent, an organization must still be able to show that the consent was obtained in a demonstrable manner. Thus, an organization must be able to prove that consent can be inferred (deduced) from another behavior on the part of the person. Such implied consent may be more difficult for the organization to demonstrate, in contrast with express consent.

[A priori compliant practice]

Example 37.1 - A company that purchases and sells automotive parts wishes to purchase insurance (a contract covering theft and fraud of company property by employees). The company must obtain the credit history of every employee who

will be covered under the insurance contract in order for it to enter into the contract. The company consults the employees concerned to ascertain their comfort in signing up for this contract. The company explains to employees that the contract would entail the verification of such employees' credit reports with their name and address once, within five working days. The company asks employees] orally whether they wanted to be covered by the insurance contract. This is the only question employee's answer. **When employees accept coverage, as they have been properly informed, they also implicitly consent to the disclosure of their name and address to the company's bank and to the collection of their credit report from the bank.**

38. **Additional criteria.** Additional criteria must be satisfied for consent to be considered valid, even when consent is implicit. Consent must therefore remain free, informed, specific, etc. In particular, relying on implied consent cannot be used as a pretext for reducing the amount of information regarding the processing activities involving his personal information.

39. **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.

2.2. Consent must be free

40. **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 their will without being unduly influenced or suffering disproportionate harm.

41. **Fair mechanisms.** It must be as easy to provide one's consent as it is to decline providing it. These options (of providing or not providing consent) must 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 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 can usually only be requested once for the same purpose, unless a substantial change in context justifies it.

[A priori compliant practice]

Example 41.1 - A municipality makes a mobile application available 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 organization has the “I accept” and “I refuse” options at exactly the same height, each placed in a button of the same color and in the same font size. **By ensuring fairness in the visual presentation of choices, it ensures that the free nature of the consent obtained is not compromised.**

[A priori non-compliant practice]

Example 41.2 - A clothing store website allows customers to create an account to facilitate online shopping. Each time you log in, it displays a pop-up window that offers the customer the weekly newsletter from the store, 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 requests for consent, without regard to the wishes already expressed by the client, may compromise its free character. Such practices are not encouraged, as the validity of such consent could be challenged**

42. **Consent as a condition.** To ensure that free consent is obtained, an organization should generally avoid presenting it as an indispensable component of the conditions of use of a service, provision of a good, or access to employment. As a reminder, consent is presumed for use and disclosure for primary purposes if the individual provides his or her personal information after being duly informed (ARA, section 65.0.2; ARPPIPS, section 8.3; see section 14). When consent is requested, it is therefore generally for secondary purposes, which should be able to be refused without impacting the original terms.

    If the act for which consent is required is necessary for the provision of a product or service, or for access to employment, the organization must make this explicit and explain the consequences of not carrying out the act. It must also be able to demonstrate why the act is necessary in the circumstances.

    [A priori compliant practice]

    Example 42.1 - In its application form for prospective students, a public university explains that personal information collected will be used to assess the application, to create a permanent code, and to communicate student status to the appropriate department, in the case of international students. It further states that providing the information requested in the form constitutes deemed consent for these purposes, pursuant to section 65.0.2 of the ARA.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.**

[A priori non-compliant practice]

Example 42.2 - 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.**

43. **Change of purpose.** Where an organization pursues a new purpose that requires consent of persons concerned by personal information (see paragraph 58), 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 previous paragraph; see also paragraph 15).

44. **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 must 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.

[Practice whose compliance may vary depending on the context]

Example 44.1 - While performing an nvestigation at a food company, members of an inspection team within government agency with surveillance functions is photographed by their supervisor, who wishes to include the image in the intervention report. The company being inspected has been in the spotlight for several months, and the media are interested in the inspection carried out by the agency. Following a media request, the supervisor who took the photo] sends an email to the relevant employees, asking them if they agree to have the photo sent to a journalist and used in his article in the paper edition of the newspaper the following day. **Given the power dynamic between the manager and their employees, the manager must be cautious. If employees feel compelled to consent to this communication, consent cannot be considered free. It must therefore be as neutral as possible in its application and must not give rise to any negative consequences for a possible refusal to communicate.**

[A priori compliant practice]

Example 44.2 - A hospital 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. Upon completion of the Privacy Impact Assessment, the hospital's Committee on Access To Information and the Protection of Personal Information approves the acquisition of a biometric system and reports the creation of a biometric bank to the CAI. In the consent form attached to the report, the hospital explains the purpose of the system and indicates that employees who do not wish to have their biometric information collected will be able to authenticate themselves using other means. For instance, 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 hospital 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.**

45. **Link to the criteria of granularity.** Consent is free only if it is requested separately for each purpose (granular; see section 2.5). The person concerned must not only have the choice of accepting everything or refusing everything.

46. **Withdrawal of consent.** Consent that is free is also consent that can be withdrawn at any time by the person concerned. While in some cases consent can be presumed (ARA, section 65.0.2; ARPPIPS, section 8.3), and accordingly where the free nature of the consent has not been assessed, consent may still be withdrawn, as provided for by law (ARA, section 65; ARPPIPS, section 8). An organization must provide a simple and accessible mechanism for withdrawing consent and must 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.

[A priori compliant practice]

Example 46.1 - 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 the same subject 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 principal investigator. **This withdrawal mechanism is simple and accessible. It does not constitute a barrier to obtaining free consent.**

[A priori non-compliant practice*]*

Example 46.2 - 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. Believing that these recommendations prevent them from discovering music by themself while exploring the platform, a user decides to withdraw their 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.**

2.3. Consent must be informed

47. The informed character of consent. 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.

48. Capacity of the person concerned to provide consent. In order to be informed, consent must first be given by a person who is able to bind themself at the moment when they manifest their consent (*Civil Code of Quebec*, article 1398). For example, consent given by an incapacitated person or a person under the age of 14 (ARA, sections 53.1 and 64.1; ARPPIPS, sections 4.1 and 14) is not valid. In such circumstances, consent may, however, be provided by a representative, such as the holder of parental authority or another representative.

49. Information to be provided. In order for a person concerned to be able to understand what they are being asked to consent to, they must be able to access the following information (which is, in many cases, similar to what information organizations must provide when collecting personal information (ARA, section 65; ARPPIPS, section 8)):

a) Who? The organization on whose behalf consent is sought;

b) Why? The purpose of the consent request, i.e. the purpose of the intended use or disclosure of the information;

c) 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;

d) With whom? Where applicable, the names or classes of third parties outside the organization from whom the organization will collect the information;

e) What? Relevant information, or at least classes 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? Period of validity of the consent;

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

i) With what risks? Reasonably foreseeable risks or consequences associated with the activity for which consent is obtained, if any;

j) How? Means of using or disclosing the information (e.g. mail communication; use of a fully automated decision);

k) Where? Location where the information will be disclosed or stored in the context of activity for which consent is obtained, 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 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: _____ . **" 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.

[Practice whose compliance may vary depending on the context]

Example 49.2 - 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:

- Platform A: "*I agree that [the Company] will share my contact information with partners*."
- 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, since Platform A does not disclose the purpose of the communication and does not give any indication as to the identity of its partners.

50. Accessibility of information - levels. Providing too much information at the same time to a person concerned can lead to confusion. Nevertheless, all of the information listed in the previous paragraph serves to ensure that consent is informed. To avoid creating an information overload in the request for consent, it may be advantageous for an organization to structure the information in several levels, taking into account the context of its activities. For example, you can prioritize information into two levels:

a. **First level**: information that can be accessed immediately and effortlessly, directly in the consent request.

i. As a minimum, the **name** of the organization (who), the **purpose** (why), an indication of **third parties**, if any (to whom/from whom), should be mentioned in this first level, as well as the **information or categories of information concerned** (what), when possible. This level should also include elements that may come as a surprise to the person concerned (long validity duration, use of uncommon technological means, numerous or significant risks, etc.);

b. **Second level**: additional information that is easily accessible through minimal effort. In oral terms, this second level may consist of a statement indicating that more information can be obtained on request. In written terms, this second level could consist, *inter alia*, of:

i. A privacy policy accessible available through a highlighted link, particularly when the written terms are displayed via technological means (LAI, section 63.4; ARPPIPS, section 8.2);

ii. An annex 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 *centre de services scolaire* (CCS) 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 CCS 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 CCS. **To ensure that such consent is informed, the CSS uses the following text, which includes all essential information in the consent request:**

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?]**. *Your consent is only valid until the certificate is actually transmitted by Police Service X* **[until when?]**. *If you refuse, we will not be able to respond to your application* **[and if not?]**. *Additional information is available in Annex A.*

☐ *I accept* / ☐ *I refuse*’.

Annex A provides the additional information, including information on the right to withdraw consent, the right of access to one’s personal information and the right to 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 is obtained through the electronic portal available on the firm’s website. 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. 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, storage location, risks, explanations on the right to withdraw consent, the right of access to personal information, the right to rectification, as well as the contact details of the privacy officer). **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.**

51. **Precision and clarity of the terms used.** The elements presented above should allow for specific consent (see section 2.4) through the provision of simple and clear terms (see section 2.5). 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.

52. **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:

    a. All information required to meet its transparency obligations regarding collection, including the primary purposes for which it collects information (ARA, sections 65 and 65.0.1; ARPPIPS, sections 8 and 8.1);

    b. 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 2.5 and section 2.8 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.

[A priori compliant practice]

Example 52.1 – 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*," the university provides a separate page requesting consent to allow the complaints office to discuss the complaint with the department's management. It sets out specific information in relation to this request for this additional consent. **By providing the new information separately from the information needed to process the complaint, the university promotes informed consent to the disclosure.**

53. **Availability of information.** Since consent that is free may be withdrawn, the person concerned must have access to the relevant information even after their consent, so that their decision (to withdraw their decision to consent) can be reassessed, if necessary. Thus, an organization must deploy means to make such information readily available.

54. **Duty to assist.** An organization should 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.

[A priori compliant practice]

Example 54.1 - 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. The organization also offers the possibility of speaking with an agent over the phone, and provides a toll-free number that is accessible during business hours. **These mechanisms are part of the organization's toolkit allowing it to provide assistance seeking to understand the scope of consent being sought.**

2.4. Consent must be specific

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

56. **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.

[A priori non-compliant practice]

Example 56.1 - A school obtains parental consent for so that a multidisciplinary team at the school may share information on a child's progress with a health facility where the child has been receiving complementary services. The school asks parents to consent to "*any information deemed necessary*" 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) to be achieved, i.e., in this case, enabling the child to receive better support from the health institution where they receive complementary services. The school should also provide details of the information involved and the expected frequency of communication, as well as the intended categories of recipients (e.g. '*professionals assigned to follow-up with the child in health facility X*').

[A priori non-compliant practice]

Example 56.2 - 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. "*staff training*", "*training artificial intelligence to automate certain steps of the grievance process*", etc.).

57. **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. Any misuse of personal information, which occurs when an organization uses or communicates information in an unauthorized manner, that deviates from what the person concerned consented to, and/or from the purposes stated at the time of collection (unless an exception is provided by law, including for consistent purposes), is a risk to the privacy of the person concerned and is deemed a confidentiality incident (see paragraph 16).

[A priori non-compliant practice]

Example 57.1 - 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 within the company. 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.**

[A priori non-compliant practice]

Example 57.2 - A person who purchases a television and a computer online agrees to the retailer providing the person's contact and purchase information to three corporate partners (who are specifically named), so that they may send promotional offers to the person. Two months later, the retailer establishes a business relationship with two new partners, and transmits the person concerned's contact and purchase information to these new partners. **The retailer cannot make such a transmission under the consent given initially, since it was specifically targeted at previous partners.**

58. **New consent for new purposes.** Where an organization wishes to use or communicate personal information for purposes other than those which individuals already consented to, the organization must obtain new consent from the individual, unless a an exception is provided by law and is applicable (see paragraphs 9 to 13).

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

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

60. Limited scope. In order for the criterion of granularity to be met, an organization must ensure that the scope of consent is defined as narrowly as possible as regards the purposes for which consent is sought. In other words, if there are multiple purposes for which consent is being sought, an organization must request consent for each purpose separately. Granularity ensures that consent is truly free. Consent is not free if the person concerned must accept several purposes at the same time. The person concerned's only choice, then, is to refuse or accept in omnibus, which does not capture the nuances of the person's will, which they may desire to express. In the same way, granularity ensures that the person concerned clearly expresses their will for each specific purpose.

[A priori non-compliant practice]

Example 60.1 - 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.

[A priori compliant practice]

Example 60.2 - A not-for-profit organization 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, allowing candidates to accept or reject these three purposes separately:**

> *"**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*"

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

61. Comprehensible character of consent. 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. 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 paragraphs.[4]

62. 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

[4] The principles of plain-language web writing in Québec.ca's government design system is a useful resource: https://design.quebec.ca/contenu/principes-redaction/langage-clair-simple.

periphrases. Text or sentences that are too long interfere with the understanding of the persons concerned.

[A priori compliant practice*]*

Example 62.1 - 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*."

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.

63. Simple vocabulary. An organization should use simple terminology, that is, terms that are accessible to the persons concerned. It should use common vocabulary items, 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 (that can be exchanged for discounts) on each purchase. Customers can view their purchase history from the last year in the store's mobile app. The grocery store decides to roll out a personalized discounts system, based on the buyer profile of customers, which the store wishes to determine on the basis of transaction history. To do so, it will seek the consent app users by using the following text:

> *"**Receive personalized offers** - By ticking "Yes," 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."*

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** - By ticking "Yes," 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 loyalty app.* ☐ ***Yes*** ☐ ***No***"

64. **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.

[A priori compliant practice]

Example 64.1 - 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 [...]".

The Committee also notes that, on web interfaces, explicit options to accept or refuse consent are not situated on the interface. In several cases, the options proposed are "*Next*" or "*Ignore*", while in other cases, the formulation of the options emphasizes acceptance at the cost of refusal. For example, an overlay window for consent window allows users to select "*Yes*" or "*Maybe Later*". **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.

65. Adaptation for public consumption. Information should be tailored to the intended audience. An organization needs to consider the perspective and profile of persons concerned: they may not have background information on their privacy rights and may not be familiar with the organization's activities, and some may not be fluent in the language used (whether spoken or written). An organization should also tailor the terms used to the lowest level of literacy among the different categories of persons concerned, for whom a request for consent is addressed.

[A priori compliant practice]

Example 65.1 - 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 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.

[A priori compliant practice]

Example 65.2 - 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 around 100 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 most of its clientele. **In this way, the company ensures that the terms are simple and clear to the audience involved.**

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

66. 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.

67. Limitation of duration. The duration limit can be linked with two types of conditions:

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

b. An event: the purpose can be considered as having been achieved 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.

[A priori compliant practice]

Example 67.1 - As part of its hiring process for professionals, an organization asks candidates to provide two references, for the purposes of assessing the quality of 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. **In order for consent to be temporary, the organization specifies that it is valid only until a decision on the application is made. This consent is therefore limited in duration by an event.**

68. Link to the specific and informed nature of consent. In order to be able to provide informed and specific consent, persons concerned must be informed of the duration of validity of their consent. Again, vague or imprecise terms should be avoided. If the end of consent validity is linked to an event, an organization should provide sufficient information to the person concerned to enable them to know the likely duration of their consent or to estimate when it might end. The organization should also inform the person of their right to withdraw consent at any time (see paragraph 49).

[5] The CAI is not responsible for the enforcement of this law.

69. **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 should remind persons concerned, at appropriate intervals, that the basis on which the organization uses or discloses the person's information is consent, and should refer to up-to-date information on this situation (see paragraph 53). It should also remind persons concerned that it is possible to withdraw consent at any time. The organization may also disseminate this information through easily accessible means (e.g., a website), which may be useful, *inter alia*, where it is not possible to reach the persons concerned.

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

70. **Distinct nature of consent.** 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, broader privacy policies, requests to confirm the validity of information provided, commitments, signatures, etc. The request for consent must 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.

71. **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. This, since the intentions behind the gesture are inseparable (see paragraphs 35 and 42). 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.

[A priori non-compliant practice]

Example 71.1 - 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 insurer....*
>
> *4. I undertake to provide notice to the order when [...].*"

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:

*"**Consent.** I agree that the order will disclose my information to the group insurer.... ☐ 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 [...].*"

[A priori non-compliant practice]

Example 71.2 - 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.

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.

BLG UNOFFICIAL TRANSLATION – 2023-06-08