NEWPORT THOMSON

WHITE PAPER

Guidelines regarding valid consent

On May 16, 2023, the *Commission d'accès à l'information (CAI)* published draft guidelines ("Guidelines") regarding valid consent under the recently updated public (ACT RESPECTING ACCESS TO DOCUMENTS HELD BY PUBLIC BODIES AND THE PROTECTION OF PERSONAL INFORMATION) and private (ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR) Quebec privacy acts affected by Law 25 (formerly known as Bill 64) .

The consultation period ended on **June 25, 2023**

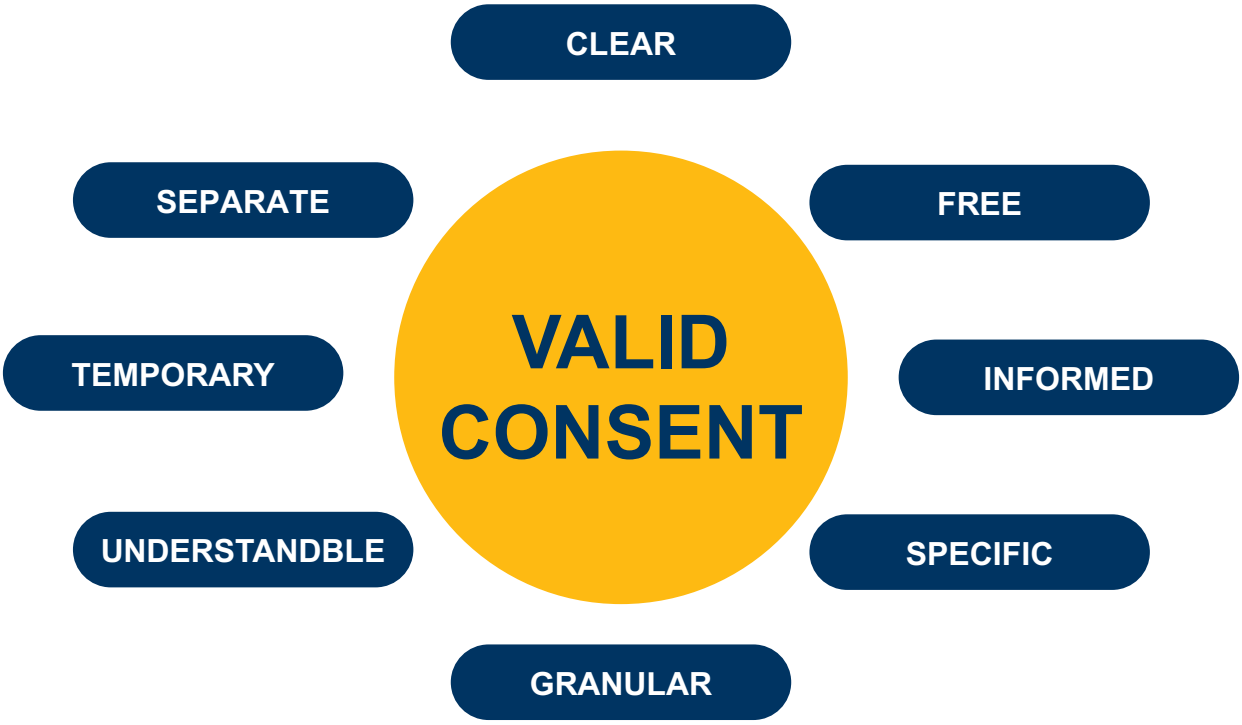
Guidelines regarding valid consent

While these guidelines are not part of either law or embedded in the additional Regulations, they do reveal what the CAI considers VALID CONSENT for the use or personal information of Quebec residents.

It is important to note that an organization does not have to have offices in Quebec for this law to apply. According to Statistics Canada, 22.5% of Canada's population resides in Quebec, therefore any organization maintaining a truly National database of Canadians must comply.

What is Valid Consent

The CAI's proposed guidelines already mentioned state:



“Consent under this Act must be **clear, free and informed** and be given for specific purposes [i.e. **Specific**].

It must be requested for each such purpose [i.e. **Granular**], in clear and simple language [i.e. **Understandable**].

If the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned [i.e. **Separate**].

If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested [this is another aspect of consent being Informed].

The consent of a minor under 14 years of age is given by the person having parental authority or by the tutor. The consent of a minor 14 years of age or over is given by the minor, by the person having parental authority or by the tutor.

Consent is valid only for the time necessary to achieve the purposes for which it was requested [i.e. **Temporary**].

Consent not given in accordance with this Act is without effect.”

Let’s dig in to understand each of these 8 elements, as we believe this will be the standard for consent that the CAI uses to enforce these new acts.

CLEAR

Consent must be clear and granted in a manner that demonstrates the true will of the person concerned. The person is aware that they are giving consent, in particular so that they understand the disclosures made by the organization concerning the handling of their personal information.

An active and unequivocally positive gesture is required.

Some Implied Consent is allowed but the CAI strongly encourages explicit consent. Explicit consent is mandatory when using sensitive data.

Cookies should be set to default “off” and allow the consumer to activate if they wish.

FREE

Consent involves genuine choice and person control, and must be given without coercion or pressure.

Cannot repeatedly ask for consent until they submit.

Cannot simply list it as “necessary to fulfill a contract”.

Must explain in plain language why it is necessary.

Consent must always be revokable - opt-out is as easy as signing up.

Be aware of balance of power - ie. employer/employee

NEWPORT THOMSON

INFORMED

Who?: the identity of the organization on behalf of whom the consent is requested

Why?: the purpose(s) for which the consent is sought

For whom?: if applicable, the name or categories of third parties to whom the personal information will be communicated

From whom?: if applicable, the name or categories of third parties from whom the personal information will be collected

What?: what (categories of) personal information will be collected

Accessible by whom?: categories of individuals within an organization who will have access to the personal information

For how long?: duration of validity of consent

Consequences of withholding consent?: these must not undercut the notion that consent should be “freely” given

Risks?: what risks or consequences in relation to the personal information are reasonably foreseeable and associated with the proposed use of such information

How?: how will the personal information be used

Where?: where will it be hosted

What rights?: explanations of right to withdraw consent + rights of access and rectification

SPECIFIC

Must be of age to consent (14+ years old)

For specific purposes, meaning that such purposes are precise and circumscribed, making it clear to the person exactly what they are consenting to

If an organization wants PII for multiple purposes, each purpose needs to be sought on its own. Think about the data use and be specific in your consent statements.

Do not use vague or ambiguous language.

GRANULAR

Consent must requested for each purpose. To meet this element, an organization must ensure that the purpose of the consent is as well-defined as possible.

If an organization intends to collect personal information for multiple purposes, the organization should separately request specific consent for each purpose.

For example, a charity fundraising for three distinct purposes:

a) to send a post-event satisfaction survey;

b) to send an info-letter; and

c) to permit the organization to send photos of the event.

According to the CAI, in order to obtain valid consent, the non-profit would have to ask the individual three separate consent questions (one in relation to each purpose of collection).

Automation may well be the only realistic solution, rather than having multiple employees handling various consents.

UNDERSTANDABLE

The request for consent must be presented in simple and clear terms, both in respect of the information and the specific statement of acceptance or refusal.

The request for consent must be concise, direct, and tailored to the level of literacy of the person concerned.

The request for consent must also be structured in several levels, taking into account the context of the organization's activities, to avoid overloading the person with information and to facilitate their understanding.

TEMPORARY

Consent is valid for a limited period of time. It is valid only for as long as is necessary for the purposes for which it was requested.

This consent is no longer valid once these purposes have been fulfilled, which can be measured by a specified term (by the passage of a certain amount of time) or by the occurrence of a certain event.

In order to provide informed and specific consent, persons must be informed of the period of validity of their consent.

Consent must always be easy to withdraw and if collected for a long period of time, the organization must periodically inform them of their right to withdraw at any time.

SEPARATE

The request for consent must be separate, that is, it must be submitted separately from any other information if it is made in writing.

Not to be confused with another action taken by the person, such as confirming that the terms and conditions have been read or that the information provided is valid.

The request for consent must be presented separately rather than embedded in a privacy policy, a Terms of Use statement, or any another document. Just because they signed up for a webinar we cannot then assume and add them to our promotion list without seeking separate consent to do so.

What every organization should do

Create new processes - to immutably PROVE consent at a specific moment in time. Most investigations require us to go back 6 or 12 months and prove consent for a specific individual on a specific date. These new practices should quickly and easily demonstrate compliance and allow an immediate response to any Order to Produce. Brands who have been fined to date report that the process of responding to the Order to Produce was more costly than the fines. It took many people away from their primary tasks and used a tremendous amount of resources. Having an automated solution that works in the back ground and can be easily searched may be invaluable to any organization.

Minimize the personal information you collect and use. Explore other ways to accomplish your business goals without relying on PI, in particular, assess the Sensitive Data you collect and use as it is held to a higher standard than data you can easily find on the internet. If that same data is require for another purpose in the future, fresh consent must be requested for that specific purpose.

Organizations should **avoid over-collection** and apply a reasonableness test to authentication practices. So collecting a copy of a valid Driver's License when authenticating an individual's identity is an over-collection. Recording that their proof of identity was shown to a staff member is all that's required. Collecting an actual copy adds to the personal information the organization has to protect. If it is collected to prove ID, that is all it can be used for.

Create clear retention rules for every field of PI collected, stored, processed or shared – set and operationalize clear retention strategies for all personal information, only keeping it to serve the purpose stated and deleting it once that purpose has been accomplished

Change your language – when asking for consent reveal all the CAI is asking for in the 8 elements above. For example (thanks Denton's);

> ***The Old Approach***
> *WidgetCo may use your personal information for marketing purposes and to improve your shopping experience. To do this, we may provide your personal information to our trusted service providers.*

Most organizations then stored that information just in case they needed to use it for something else in the future. That is now a violation of the new laws.

> ***New approach***
> *WidgetCo uses your name, address, email address and phone number to send you marketing emails. We provide your information to use [Service Provider X] which helps us send these communications. These service providers are located in the United States. Our marketing team and other authorized individuals have access to this information. We keep your information as long you have an account with us and for [X] months thereafter, in order to support our documentation requirements. If you do not wish to consent, we will be unable to deliver our marketing materials and you may miss out on discounts or sales.*

We use your browsing history and shopping history to deliver ads targeted to you as you move across websites. We provide your information to use [Service Provider X] which helps us deliver these ads. Our marketing team and other authorized individuals have access to this information. We keep your information as long you have an account with us and for [X] months thereafter, in order to support our documentation requirements. If you do not wish to consent, we will still deliver online ads, but they may not be relevant to you.

Organizations must provide individuals with enough information for them to give informed consent. However, they must not confuse individuals by providing them with too much information. Once an individual declines to consent to the collection, use of communication of PI, an organization cannot rely on an applicable exception instead.

Establish necessity: Personal information can only be collected, used or communicated where necessary

Consent doesn't override necessity: The necessity requirement must be met even if an organization obtains consent or if an exception to consent obligations applies

In September 2022 a few elements of Law 25 came into force, including Confidentiality Reporting Planning requirements. A failure to obtain and prove valid consent **is a privacy breach and must be documented and entered into the Log of Confidentiality Incidents**, which must be updated for every incident and made available to the CAI upon request. Documentation and demonstrating compliance is an ongoing requirement of Law 25. If valid consent cannot be proven the CAI will not consider it valid, resulting in fines and an order to come into compliance, in addition to the public shame involved.

Do not bundle consent with Terms of Use or your Privacy Statement.

Summary

In anticipation of these kinds of data protection & privacy laws over the past 10+ years we have been scouring the internet for powerful but flexible SaaS models to manage consents of all types so our clients could actually implement a Consent Management initiative with ease. We found two that we actually use ourselves:

- **RAVEN by DRT Cyber**
  https://drtcyber.com/

- **CASSIE by Syrenis**
  https://trustcassie.com/

Vendor Overview

RAVEN by DRT Cyber

When the Canadian Anti Spam Legislation (CASL) was introduced it included a requirement for organizations to prove consent (implied or express) before sending an Commercial Electronic Message or CEM (an email or SMS Text message). Newport Thomson not only wanted compliance, we wanted to tickle our audience pink, so we put RAVEN to work for us.

Any individual using a newportthomson.com email address must “manage” consent before the system will allow them to send an email (we do not SMS text anybody as Newport Thomson). A common misperception about CASL is it only impacts the sending of bulk, promotional emails such as newsletters or updates, when in fact one-to-one emails are considered a CEM and consent requirements apply.

CASSIE by Syrenis

Cassie is one of the most powerful consent management solutions available around the world. Flexible and highly configurable, Cassie adapts to the way your organization works so that you don’t need to change your processes or workflows. Consent management starts with your consumer: Cassie enables them to have granular control over their preferences. If they change their mind, they can simply log in and change their settings.

As part of the set-up process, Cassie connects to all the places you use data for centralized consent management. For example, if you use email marketing automation tools like MailChimp, Cassie can connect via API to continually update the platform about individual consent status. This ensures customers and prospects only receive emails they have given consent for, meaning they’re more likely to engage and convert. All types of consent can be managed and operationalized using Cassie.

Every country has different data protection and privacy laws. Your organization cannot take a one size fits all approach and expect to remain competitive or compliant. To manage global compliance, an organization can deploy Cassie centrally but allow for local business rules. For example, when a consumer logs in from an IP address in California, they are presented with language and options that comply with CCPA/CPRA. Once set up is complete, Cassie works seamlessly in the background to manage consents in real time, ensuring accurate communication and compliance across your tech stack.

Want to find out more?

For a demo of RAVEN or CASSIE contact:

Call for help:
(416) 524 7844

Email for information:
info@newportthomson.com

Head office address:
4800 Dundas Street West, Suite 100, Toronto, Ontario M9A 1B1

Trusted Privacy Advisors

Documenting Compliance

Staff Privacy Training

Automating Privacy