2727 COWORKING / RESEARCH & PRACTICAL GUIDANCE

AI Note Taker Meeting Room Consent in Montreal: Checklist

> Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Published by 2727 Coworking · 2026-11-15 · ai note taker meeting room consent montreal · ai meeting transcription consent quebec · recording a meeting in quebec · law 25 ai meeting transcripts · teams external bots · meeting room microphone setup · transcript retention · montreal meeting room rental · ai note taker privacy checklist

Original article: https://2727coworking.com/articles/ai-note-takers-montreal-meeting-room-consent-checklist



In this article

1. Executive Summary
2. Introduction and Background
3. Key Changes Shaping the Decision
4. The Room Audit: Physical Audio Path
5. Choosing a Documentation Mode
6. Implementation Considerations and Process Changes
7. Data Analysis and Evidence
8. Implications and Future Directions
9. Frequently Asked Questions (FAQs)
10. Conclusion

Executive Summary

A Montreal freelancer, agency or 2 to 12 person hybrid team that books a meeting room for a client review, team discussion or interview has four documentation options: **human notes**, an **approved platform transcript**, a **third-party meeting bot**, or **no recording**. The evidence reviewed supports a sequence rather than a single answer. First test whether a transcript is needed at all, because the Commission d'accès à l'information du Québec (CAI) states that the necessity criterion takes precedence over consent (www.cai.gouv.qc.ca). Then choose a mode, audit the room, and record who holds the resulting files.

Consent, where required, must be informed (CAI consent guidance: informed) and requested for each specific purpose (CAI consent guidance: specific purpose), and consent to sensitive information must be expressed explicitly (CAI consent guidance: sensitive information). The federal Criminal Code exempts an interception made with the consent of the originator of the communication (laws.justice.gc.ca), but that exception does not replace business privacy duties, client contract terms or employment rules. Quebec's private-sector Act also requires a written agreement and an assessment before personal information is communicated outside Quebec (www.legisquebec.gouv.qc.ca), so "stored in Canada" does not settle where processing happens.

Platform controls help but prove nothing about consent. Microsoft Teams places detected external bots in the lobby irrespective of lobby configuration (learn.microsoft.com), yet Microsoft documents that some external bots may not be detected (learn.microsoft.com). Voice identification is a separate layer: in-room participants can be distinguished without any biometric identification (learn.microsoft.com), while the federal commissioner says recording that involves biometric voiceprints may call for express consent (www.priv.gc.ca).

The room matters as much as the software. A sound leak equal to one-tenth of one per cent of a partition area limits effective Sound Transmission Class (STC) to about 30 (web.mit.edu), and Government of Canada guidance names door leakage as the primary cause of failure to achieve high speech privacy (grc.ca). Neither an enclosed room nor a platform notice proves that a meeting is private or legally authorized. This report supplies a one-page go/no-go sheet, a bilingual opening script, a custody inventory and a synthetic-audio rehearsal. No provider or room was tested, no 2727 room configuration is claimed to be soundproof or approved for regulated work, and unresolved vendor or cross-border questions belong with a privacy owner or lawyer.

Introduction and Background

Meeting rooms are rented for conversations that carry commercial weight: a client reviewing a draft, a founder interviewing a candidate, a manager working through a team disagreement. Software that records or transcribes speech and produces notes (an "AI note taker") can turn such a conversation into a durable file that outlasts the booking. This report examines the decision a small Montreal team faces before the door closes: human notes, an approved platform transcript, a third-party bot or no recording, and whether the particular room and microphone setup suits that choice.

The scope is deliberately narrow. It is not a comparison of AI productivity tools or a general Law 25 checklist. Its contribution is one approval sheet that joins the physical audio path (doors, corridors, ceilings, microphones, bystanders) to the digital custody of what the software produces (recording, transcript, summary, exports). A Canadian law firm's November 2025 overview names the same cluster of concerns: privacy, data security, employment and intellectual property (www.nortonrosefulbright.com). That overview is professional guidance, not a measured benchmark.

Three kinds of evidence are kept apart. **Official guidance** (the CAI, the Office of the Privacy Commissioner of Canada, statutes) frames duties. **Documented vendor controls** (Microsoft, Google, Zoom and note-taker help pages) describe what software can do; they are technical controls, not consent determinations. The **checklist** is a working proposal: no benchmark tests whether it improves outcomes, and no adoption or time-saving statistic is offered because none was found from a primary source. Confirm scope, license, tenant policy and settings in the actual account.

A disclosure on perspective: the publisher, 2727coworking.com, is a Montreal coworking and virtual-office provider that rents desks, private offices and meeting and conference rooms. It is a direct provider of the room category discussed and makes no price or performance claims here, and no claim in this report relies on its own pages as evidence. This report is not legal advice and has not been reviewed by a lawyer.

Key Changes Shaping the Decision

Platforms now identify and gate third-party bots

Microsoft's Teams documentation states why the control exists: external meeting assistants may record or transcribe meetings without participant awareness (learn.microsoft.com). When detection is enabled, detected bots are placed in the lobby irrespective of lobby configuration (learn.microsoft.com). Registered vendors can add a self-identification marker to their join requests (learn.microsoft.com), and the Bot Identification Program is described, in a page updated in August 2026, as a public preview that has reached its current bot provider capacity (learn.microsoft.com).

Three limits matter for a small team. First, the policy is a tenant setting (learn.microsoft.com), so the organizer's account, not the rented room, decides; a freelancer joining a client's meeting is governed by the client's tenant. Second, Microsoft lists as a known limitation that some external bots may not be detected (learn.microsoft.com). Third, detection relies on signals collected during the meeting join process (learn.microsoft.com). That describes software that joins a meeting, not a recorder running on a participant's own laptop, and vendors document such modes: Otter's desktop app records without a notetaker joining as a

participant (help.otter.ai), and Granola states that it captures audio from the device so no bot joins the call (docs.granola.ai). These are documented designs, not criticisms; they mean the lobby is one control among several. For sensitive meetings Microsoft suggests having all participants wait in the lobby until an organizer or co-organizer admits them (learn.microsoft.com). This report does not state any rollout date for newer bot options, because technology-news coverage is not a primary source.

Quebec law puts necessity before consent

The CAI's consent guidance begins with a sequencing rule: necessity takes precedence over consent (CAI consent guidance), and necessity goes beyond mere usefulness (CAI collection guidance). For a meeting, the test is whether the purpose (an accurate action list, a record of client instructions) could be met by a less intrusive means such as a human note taker. If so, a transcript may be convenient but not necessary, and consent cannot cure that.

Where collection is justified, consent has defined qualities. The Act says consent must be clear, free and informed and given for specific purposes (Quebec private-sector Act, consent), and valid only for the time needed to achieve them (Act, duration of consent). A bot notice buried in a calendar invitation sits uneasily with those qualities. Consent for sensitive information must be expressed explicitly (CAI guidance on sensitive consent), and the CAI explains that information is sensitive when it creates a high degree of reasonable expectation of privacy (CAI definition of sensitive information), so a client review touching health, finances or personnel matters can be sensitive by context.

Scope needs care. The CAI says the Act targets persons who operate an enterprise in Quebec (CAI scope guidance), and the Civil Code defines that as an organized economic activity, commercial or not (Civil Code of Québec, definition of enterprise). That suggests, as an inference and not a sourced ruling, that a freelancer or small agency serving clients is likely within the Act. At collection, people must be told of their right to withdraw consent (Act, right to withdraw), and technology with functions that allow a person to be identified, located or profiled requires advance notice (Act, identification technologies) and cannot be activated by default (CAI collection guidance, default settings). Neither the Act nor the CAI pages reviewed say whether a meeting bot, speaker labelling or an AI summary is such a technology; that interpretation is flagged for the privacy owner.

Civil law adds a separate layer. Every person has a right to respect of reputation and privacy (www.legisquebec.gouv.qc.ca), and intentionally intercepting or using private communications is listed as an invasion of privacy (www.legisquebec.gouv.qc.ca). These texts state no consent formula for meeting recordings; they are reasons to treat recording as privacy-sensitive.

The federal interception rule is a narrow exception

The Criminal Code makes it an offence to knowingly intercept a private communication (laws.justice.gc.ca). "Intercept" includes to listen to, record or acquire a communication (laws.justice.gc.ca). Section 184(2)(a) exempts a person who has the consent, express or implied, of the originator (laws.justice.gc.ca) or of the person the originator intended to receive it (laws.justice.gc.ca), and where there are several originators or recipients, consent from any one suffices for that part of the Code (laws-lois.justice.gc.ca). A Quebec law firm summarizes the corollary that a person may record their own conversation with someone else (langlois.ca); that is a firm's summary, not a statute.

This answers a narrow question: whether the recording is a criminal interception. It does not answer whether a business may collect, keep, share or reuse the content. The federal commissioner's customer-call guidance treats consent as implied when the customer proceeds knowing the call is recorded and why (www.priv.gc.ca), but says recording involving biometric voiceprints or other sensitive information may call for express consent (www.priv.gc.ca). It adds that the purpose should be stated as clearly and narrowly as possible (www.priv.gc.ca) and that the information may only be used for the purposes specified (www.priv.gc.ca); more generally, consent should be express unless implied in strictly defined circumstances (www.priv.gc.ca). That page concerns customer calls and is persuasive context, not a rule written for Quebec meeting rooms.

PIPEDA (the federal Personal Information Protection and Electronic Documents Act) should not be applied automatically to every Quebec-only small business. The OPC explains that organizations covered by a substantially similar provincial law are generally exempt from PIPEDA for collection, use or disclosure within that province (www.priv.gc.ca), while the federal Act still reaches transactions involving personal information transferred across borders (www.priv.gc.ca). Whether a cross-border commercial flow exists is a fact to establish. Employment forms a third strand: employers must inform employees when technological monitoring measures are used (educaloi.qc.ca), so an internal discussion recorded for a manager raises questions a client review does not.

Custody: where the data goes decides the next question

The CAI says that before personal information is communicated to an entity outside Quebec, it must be shown that the information will receive adequate protection (CAI guidance on communicating information; adequate protection), and that such communication must always be covered by a written agreement (CAI written-agreement requirement). The statute carries the same obligations through a privacy impact assessment (in French, évaluation des facteurs relatifs à la vie privée, EFVP) and a written agreement (www.legisquebec.gouv.qc.ca). An EFVP is also required for projects to acquire or redesign an information system involving personal information (www.legisquebec.gouv.qc.ca), and a mandate to an outside provider must state that the provider does not keep the information after the contract expires (www.legisquebec.gouv.qc.ca). The CAI's EFVP guide develops these triggers (CAI EFVP guide). Reusing information for a new purpose generally means obtaining consent again (www.cai.gouv.qc.ca).

The wording is "outside Quebec", not "outside Canada", which is why equating "stored in Canada" with "processed in Quebec" fails. The federal commissioner reaches a consistent point: contract is the primary means of securing comparable protection (www.priv.gc.ca), yet no contract can override the laws of the country where the data sit (www.priv.gc.ca), and individuals should be told that information may be sent to another jurisdiction for processing (www.priv.gc.ca).

Vendor documentation shows why the answer cannot be generic. Fathom states that all its data is stored in the United States (help.fathom.video); Granola states that all data is stored on servers located in the United States (docs.granola.ai); Zoom says it processes and stores data based on the hosted data center region and the host's settings (library.zoom.com). These are neutral documented facts that differ by vendor and plan, and they are inputs to the EFVP, not conclusions about suitability.

Voice identification is a separate layer from transcription

Transcribing speech and identifying the speaker are different functions. Microsoft's Teams Rooms documentation describes speaker recognition that creates a voiceprint for each participant (learn.microsoft.com) and describes the feature as supported for biometric enrollment and in-meeting transcription (learn.microsoft.com). Enrollment is opt-in (learn.microsoft.com), although availability is on by default at tenant level (learn.microsoft.com). In-room people can be distinguished without any biometric identification (learn.microsoft.com). Otter documents automatic speaker enrollment using stored voice data, with a workspace setting to disable it (help.otter.ai). The OPC notes that biometric voiceprints may call for express consent (www.priv.gc.ca), and the CAI requires disclosure of biometric use (www.cai.gouv.qc.ca). The consequence is a verification step, not a label: this report does not treat all voice transcription as biometric. The sheet asks whether the specific tool actually performs voice identification or speaker learning and, if so, escalates before use (www.cai.gouv.qc.ca).

The Room Audit: Physical Audio Path

Table 1 below compares where such a meeting can occur. It describes what to verify, not what any room delivers; no source reviewed supports a claim that any Montreal room is soundproof or approved for regulated work.

Meeting location	Who controls AV and recording tools	Bleed and bystander checks	Obtain in writing before booking
Client's own office room	Client IT and tenant policy decide which bots and transcripts are allowed.	Client staff may pass or listen at the door; shared screens may show other matters.	Client written permission for the chosen mode; named privacy contact.
Café, lobby or open area	Nobody; personal devices only.	Strangers within earshot; recording by any device cannot be seen.	Generally unsuitable for confidential discussion or recording.
Rented private meeting room (any provider)	Provider supplies room and sometimes AV; the renter's account controls software.	Door gaps, glass walls, ceiling plenum, neighbouring rooms, corridor traffic, who can enter.	Equipment list, wall and door description, neighbouring-room use, operator entry rules, shared-device sign-out, itemized quote (taxes, AV, overtime).

Table 1 compares rented-room options without favouring any provider. The decision-relevant column is the right-hand one: the same written questions apply to every provider, and answers should arrive as written descriptions and quotes rather than assurances.

Sound leaving and entering the room

Acoustic ratings measure assemblies, not meetings. The STC standard says its single-number ratings correlate only in a general way with subjective impressions of sound transmission (store.astm.org), and the open-plan speech privacy standard says it is not directly applicable to privacy between open plan and enclosed spaces (store.astm.org). A closed room beside a corridor cannot be certified private from a headline rating. Historic National Research Council of Canada building digests (1964 to 1985, mirrored on a university

site) remain useful physics: speech privacy means less than about 5 per cent of transmitted speech is understood (web.mit.edu); a leak of one-tenth of one per cent of a partition's area limits effective STC to about 30 (web.mit.edu); sound may travel over a partition through the ceiling plenum (web.mit.edu); and on-site tests capture flanking paths that laboratory ratings do not (web.mit.edu).

A Government of Canada guide for sensitive-discussion rooms makes the same points in current form: leakage around doors is the primary cause of failure to achieve high speech privacy (grc.ca). It is written for government spaces, so it is an illustration, not a standard for ordinary offices, but the logic transfers: inspect the door gap, check for ceilings that run through, and treat glass and shared walls as paths.

Microphone coverage and what it does not exclude

Coverage and privacy pull in opposite directions. Microsoft's room planning guidance says microphone and speaker coverage must include every seat (learn.microsoft.com), and its device guide suggests at least one microphone within **7.5 feet (2.3 meters)** of each participant (learn.microsoft.com). Manufacturers describe pickup shaping: Shure documents up to eight configurable coverage areas (www.shure.com) and reducing unwanted sounds from other parts of the room (www.shure.com); Jabra states that its PanaCast 50 is Teams-certified for rooms up to a stated size (www.jabra.com); Logitech publishes a placement guide for add-on microphone pods (futureisnow.logitech.com). These are vendor claims about pickup, not independent measurements, and none promises that corridor speech is never captured. The sheet therefore asks for a coverage map: which seats are covered, which zones are muted or excluded, and what remains audible near the door.

Personal devices and proximity

A room is also a collection of personal devices. Microsoft warns that leaving a personal device's audio on when accepting a call on the room console can cause echo (support.microsoft.com), and that proximity join can use a Bluetooth signal that can penetrate through walls (learn.microsoft.com). For the consent question, the important point is that a participant's laptop or phone may run its own recorder, so the opening script asks every person in the room whether any device is capturing audio.

The synthetic-audio rehearsal

A rehearsal checks the setup without capturing strangers, using only the team's own scripted voices.

- **Script:** two or three known speakers read a short script with names, numbers, a French passage and an English passage.
- **Positions:** speakers sit in the seats that will be used; one reads from the far end of the table.
- **Door test:** a known speaker reads in the corridor while another listens inside, and the reverse, with the door closed.
- **Platform check:** run the platform's own test, such as the Teams test call for checking call quality (support.microsoft.com).
- **Scorecard:** record pass, fail or not tested for: seat covered, speaker attributed correctly, both languages captured, names and numbers correct, corridor speech audible inside, inside speech audible in the corridor.

- **No invented numbers:** the scorecard records observed outcomes for this room on this day; it produces no accuracy percentage.

```
PHYSICAL PATH                              DIGITAL PATH
 speakers -> room air -> door/glass/        microphone -> platform or bot
 ceiling plenum -> corridor/neighbours        -> recording / transcript / summary
 speakers -> microphones (coverage map)       -> account owner -> storage region
 personal devices (local recorders)           -> exports, copies, vendor processing
                                              -> retention, deletion, access requests
```

Choosing a Documentation Mode

Table 2 below maps purpose and sensitivity to a mode and the room conditions that accompany it. It is a decision aid built from the sources above, not a legal determination, and every row assumes the necessity test came first.

Purpose and sensitivity	Candidate mode	Room requirements	Flags for the privacy owner
Routine internal planning, no personal or client-confidential detail	Human notes, or platform transcript in the organizer's own account	Every seat covered; rehearsal done	Retention date; who can download.
Client review with confidential material	Human notes by default; transcript only with written client permission	Door and glass checked; no bystander access; screens away from the corridor	Client contract restrictions; where the client's tenant stores files.
Job interview or performance conversation	Human notes, or no recording	Entry controlled; no personal devices recording	Employment rules; sensitivity by context; express consent if the content is sensitive, otherwise clear, informed consent.
Discussion touching health, finances or other sensitive information	No recording unless necessity and express consent are documented	Rehearsal passed; door leakage addressed	Express consent; EFVP; processing location.
Third-party bot requested by an attendee	Only if pre-approved by the account owner and disclosed	Bot visible to all; lobby admission by organizer only	Vendor contract; outside-Quebec processing; secondary uses such as model training.

Table 2 shows that a transcript is a choice with prerequisites, not a default. Sensitivity pushes the mode toward human notes or no recording, and the room requirements tighten at the same moment. The bottom row exists because a third-party bot is the case where the account owner, the other attendees and the vendor are three different parties.

Implementation Considerations and Process Changes

Disclosure: a bilingual opening script

A platform notice is only part of disclosure. Teams can display a banner when recording or transcription starts, with administrator-customizable consent text (learn.microsoft.com). Google Meet shows a pencil icon to all participants while notes are taken (support.google.com) and notifies them when recording starts or stops (support.google.com), and Zoom shows an AI Sparkle icon when summaries are active (library.zoom.com) and lets participants ask the host to disable its AI features (library.zoom.com). Otter tells users to always obtain any required consent (help.otter.ai) and to notify participants before using its desktop app (help.otter.ai). These are icons and messages; none is a consent determination, and the OPC advises that consent be as specific as possible and avoid deceptive design patterns (www.priv.gc.ca).

The script below is a draft with placeholders, in English and then French. Both require legal review, and bracketed items must be completed from the facts of the actual setup.

> **English (draft):** "Before we start, we would like to [record / transcribe] this meeting with [tool] in order to [specific purpose, for example: produce a written summary and action list]. The people who will have access are [list]. The recording, transcript and summary will be kept in [account, country or region to be confirmed] for [period] and then deleted. The provider [name] may process the data in [location, to be confirmed]. You may decline without consequence; in that case we will take handwritten notes. You can withdraw your agreement at any time by contacting [privacy contact]. Does anyone object, or is any device in this room already capturing audio? [Legal review required.]"

> **Français (ébauche) :** « Avant de commencer, nous aimerions [enregistrer / transcrire] cette réunion avec [outil] afin de [but précis, par exemple : produire un compte rendu et la liste des suivis]. Les personnes qui y auront accès sont : [liste]. L'enregistrement, la transcription et le résumé seront conservés dans [compte, pays ou région à confirmer] pendant [durée], puis détruits. Le fournisseur [nom] peut traiter les données à [lieu, à confirmer]. Vous pouvez refuser sans conséquence : dans ce cas, nous prendrons des notes à la main. Vous pouvez retirer votre accord en tout temps en communiquant avec [personne responsable]. Quelqu'un s'y oppose-t-il, ou un appareil dans cette salle enregistre-t-il déjà le son? [Révision juridique requise.] »

A short glossary supports the script:

- **Consentement:** consent; the CAI requires it to be informed and specific.
- **Renseignement personnel sensible:** sensitive personal information, which needs express consent.
- **Évaluation des facteurs relatifs à la vie privée (EFVP):** privacy impact assessment.
- **Responsable de la protection des renseignements personnels:** the person in charge of protecting personal information.

Accounts, access and the custody inventory

Custody starts with the account that creates the files. Teams stores transcripts with recordings, and external participants have no recording access unless the organizer shares it (see *Table 3*). A support article says all participants see a notification that the meeting is being transcribed (support.microsoft.com). *Table 3* below turns these facts into an inventory to fill in per meeting.

Artifact	Documented location and default access	Documented retention and deletion	Evidence to keep
Audio or video recording	Teams: organizer's storage; external participants have no access unless shared (learn.microsoft.com)	Teams default expiry 120 days (learn.microsoft.com)	Owner name, location, deletion date.
Transcript	Teams: stored with the recording (learn.microsoft.com); Google Meet: organizer's Drive, following the organization's retention policy (support.google.com)	The organizer and co-organizers can delete a Teams transcript (support.microsoft.com)	Who downloaded it; deletion confirmation.
AI summary or action list	Teams recap without a saved transcript: same-organization attendees with a Copilot license (learn.microsoft.com)	Cached transcription data purged within one day (learn.microsoft.com)	Reviewer name; edits made.
Exports and downloaded copies	Wherever the downloader stored them, outside platform expiry	Granola retains notes and transcripts indefinitely unless deleted or an auto-deletion period is set (docs.granola.ai)	Download log; deletion of local copies.
Vendor-side copies and caches	Depends on region: Zoom by hosted data center (library.zoom.com); Fathom in the United States (help.fathom.video)	Zoom admins can move summaries to the Trash after a set number of days (support.zoom.com)	EFVP result; written agreement.

Table 3 is a template, not a finding about any provider. It forces an answer in each cell before the meeting: owner, users, location, retention and deletion evidence. A cell that cannot be filled from vendor documentation goes to the privacy owner. Summaries need particular care: Microsoft documents that recap can work without saving a persistent transcript (learn.microsoft.com), yet prompts and responses might be retained for compliance purposes even if recording and transcription are turned off (learn.microsoft.com). A team that equates "no transcript" with "no data" should read that page for its exact scope.

Retention, deletion and access requests

The Act requires governance policies framing the keeping and destruction of information (Act, governance policies), and destruction or anonymization once the purposes are achieved (Act, destruction or anonymization); the CAI adds that information must be securely destroyed when no longer needed (CAI destruction guidance). The federal commissioner's AI principles call for retention schedules (OPC AI principles), and its call-recording guidance advises limiting retention of recordings (OPC call-recording guidance). In Teams, a changed expiry setting affects only newly created files (learn.microsoft.com).

People have rights over what is kept. A person may demand rectification when information about them is inaccurate, incomplete or equivocal (www.legisquebec.gouv.qc.ca), which covers a wrongly attributed statement in an AI transcript. A response to an access or rectification request is due not later than 30 days

after receipt (www.legisquebec.gouv.qc.ca), and silence after 30 days is deemed a refusal (www.legisquebec.gouv.qc.ca). By default the person exercising the highest authority is the person in charge (www.legisquebec.gouv.qc.ca), and that person's title and contact information must be published on the enterprise's website (www.legisquebec.gouv.qc.ca). For a one-person business, that is the freelancer.

Human checking, bots and the approval record

Vendors document that outputs can be wrong. Google states that a meeting summary can be incomplete, inaccurate or not generated (support.google.com) and Otter recommends reviewing and editing transcriptions (help.otter.ai). Google's notes feature supports one language at a time (support.google.com), so a bilingual meeting should be rehearsed in both languages. A named person compares the action list and speaker labels with handwritten notes before anything reaches a client.

Where a bot is approved, the account owner should be the admitting party. Otter states that its Notetaker cannot join anonymously (help.otter.ai), Fireflies states that it joins as a visible participant and will not join if even one participant opts out (guide.fireflies.ai), Fathom lets admins enforce a consent chat message for bot-free meetings (help.fathom.video), and Zoom limits starting its summary to the host or co-host (support.zoom.com). The approved-bot test is: named vendor, named account owner, visible join, host-controlled admission, written vendor agreement, and a recorded answer to "where is it processed".

The sheet below joins room checks and custody checks into one record. Answer each line yes, no or not applicable before the booking is confirmed.

- **Purpose and necessity:** a specific purpose is written down, a less intrusive means was considered, and the choice of a transcript is justified.
- **Mode:** human notes, platform transcript, approved bot, or no recording is selected.
- **Client approval:** written permission is on file and no contract clause prohibits the mode.
- **Employment:** if staff are present, applicable employment rules and notice are checked.
- **Sensitivity:** the content is not sensitive by nature or context, or express consent is planned.
- **Room audit:** door, glass, ceiling and neighbouring uses are described in writing by the room provider.
- **Rehearsal and coverage:** the scorecard has no unresolved fail and the microphone map covers the seats used.
- **Bystanders and devices:** entry is controlled, and every person was asked whether a device is capturing audio.
- **Tool inventory:** native transcription, bots and local recorders are listed.
- **Disclosure:** the script is used in the participants' language, with a refusal option.
- **Account owner and access:** one named person owns the source account; users of recording, transcript, summary and exports are listed.
- **Location:** storage region and vendor processing locations are known; if data leave Quebec, the assessment and written agreement are on file.
- **Voice identification:** speaker enrollment or voice profiles are confirmed on or off.
- **Retention and vendor policy:** a deletion date is set, deletion evidence is assigned, and the vendor's privacy policy and processing terms were read and match that date.

- **Human check and requests:** a named person checks attribution and action items; a named person receives access, correction or withdrawal requests.
- **Decision:** go, no-go or escalate, with name and date. Unresolved vendor, contract or cross-border questions go to the privacy owner or a lawyer.

Room cost belongs in the record only as written quotes: ask each provider to itemize room time, taxes, AV equipment and overtime. No quotes were obtained for this report. The workload worksheet is a method, not a finding: add actual meeting minutes to transcript review, redaction, deletion administration and request handling, then compare with the actual effort of manual notes, as scenarios.

Data Analysis and Evidence

The figures below come from statutes, regulators, statistical agencies and vendor documentation. No public benchmark of transcript accuracy, adoption or time saving was found from a primary source, so none is reported.

- **Statutory timelines:** access or rectification responses are due within **30 days** (www.legisquebec.gouv.qc.ca). A Quebec government release says the Law 25 rollout began on 22 September 2022 (www.quebec.ca), and the CAI dates the new consent rules to September 2023 (www.cai.gouv.qc.ca).
- **Statutory ranges for monetary penalties and fines (text of the Act only):** administrative monetary penalties for an enterprise are capped at **$10,000,000** or, if greater, 2% of worldwide turnover (www.legisquebec.gouv.qc.ca); penal fines range from **$15,000 to $25,000,000**, or, if greater, 4% of worldwide turnover (www.legisquebec.gouv.qc.ca).
- **Teams defaults:** recordings and transcripts expire after **120 days** by default (learn.microsoft.com).
- **Acoustic figures:** one-tenth of one per cent leak area limits effective STC to about **30** (web.mit.edu); speech privacy means under about 5 per cent of speech understood (web.mit.edu). These 1964 to 1985 digests illustrate physics, not current code.
- **Hybrid-work context:** about **35%** of Quebec's labour force teleworked in 2022, with **45%** in the Outaouais and Montreal regions (statistique.quebec.ca); nationally, **17.4%** of employed people mostly worked from home and **10.0%** worked hybrid in May 2025 (www150.statcan.gc.ca). These describe where hybrid meetings come from, not note-taker use.

(Hypothetical Example) A team holds a **60-minute** client review. Assume, purely for illustration, that checking speaker labels and action items takes 25 minutes, redacting one passage takes 10, and deletion administration takes 5, for 40 minutes of transcript handling, while handwritten notes and cleanup take 30. Here the transcript route costs 10 more minutes; other inputs could reverse that. The numbers are invented to show arithmetic and are not a benchmark or forecast.

Implications and Future Directions

The sheet should be re-checked on a schedule because several parts are moving. The Teams Bot Identification Program is described as a public preview, so its scope and licensing may change, and the account's current settings are the only reliable reference. The CAI has said that AI in the workplace raises significant privacy issues for employees (www.cai.gouv.qc.ca), which signals continued attention to employer use of such tools.

For small teams the implication is governance in proportion to size: name a privacy owner (for a freelancer, themself), keep the one-page sheet with the booking, and escalate unusual cases. For room buyers, the room becomes part of the evidence: written descriptions plus a rehearsal scorecard are worth more than a general assurance. For advisers, the open questions are interpretive: whether an AI feature is a "profiling" technology, and whether a vendor's processing triggers the outside-Quebec assessment.

Frequently Asked Questions (FAQs)

Is it legal to record a meeting in Canada?

The Criminal Code exempts interception made with the consent of the originator (laws.justice.gc.ca), and consent from any one of several originators or recipients suffices for that part of the Code (laws-lois.justice.gc.ca). That addresses criminal interception only. Quebec privacy duties, client contracts and employment rules apply separately.

Is consent needed to use an AI meeting transcription tool in Quebec?

Often yes where personal information is collected, and the consent must be informed and specific (www.cai.gouv.qc.ca); sensitive information requires express consent (www.cai.gouv.qc.ca). Necessity comes first (www.cai.gouv.qc.ca). Whether a specific meeting needs consent depends on content, participants and tool.

Does Law 25 apply to AI meeting transcripts?

The Act applies to persons operating an enterprise in Quebec (www.cai.gouv.qc.ca), and a transcript containing personal information falls under its retention and access duties (www.legisquebec.gouv.qc.ca). Scope for a specific business is a legal question.

Does a Teams notice prove everyone consented?

No. Banners, icons and lobby controls are technical features, and the documented limits described above mean they cannot prove that everyone consented.

What microphone setup suits a small conference room?

Coverage should reach every seat, with a microphone near each participant, as described in the room audit. Check the manufacturer's documented coverage and exclusion options for the exact device (www.shure.com) and rehearse with scripted audio.

Is an enclosed room private enough for a transcript?

An enclosed room is not proof of privacy; door leakage is the primary cause of failure to achieve high speech privacy in government guidance (grc.ca). Ask for written descriptions and test with your own voices.

How long should a transcript be kept?

Only as long as the purpose requires: the Act requires destruction or anonymization once purposes are achieved (www.legisquebec.gouv.qc.ca), and the 120-day Teams default is a platform setting, not a legal retention period.

Which Montreal meeting rooms can be rented for this?

Any provider that supplies written room descriptions and itemized quotes can be considered, including the rented-room rows in Table 1. No room is claimed here to be soundproof or approved for regulated work.

Conclusion

Using an AI note taker in a rented meeting room is a chain of smaller decisions with different owners. Necessity comes before consent under CAI guidance. The Criminal Code's consent exception answers only the interception question. Platform controls such as the Teams lobby help but are documented as incomplete. The room's doors, ceiling, glass and microphone coverage determine what is captured and what escapes, and the digital path (account, region, vendor, retention, exports) determines who holds the result.

The go/no-go sheet joins those links with a bilingual opening script, a custody inventory and a synthetic-audio rehearsal. It is a working proposal that has not been tested at scale, and no accuracy or time-saving claim is made. Neither an enclosed room nor a platform notice proves that a meeting is private or legally authorized. Where the sheet cannot be completed, the correct outcome is to escalate to a privacy owner or lawyer, or to choose human notes. Teams that want a written room description and itemized quote can request one from the provider of their choice, including the publisher of this report, 2727 Coworking (disclosed above).

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/consentement-personnes-entreprises
2. https://laws.justice.gc.ca/eng/acts/c-46/section-184.html
3. https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1
4. https://learn.microsoft.com/en-us/microsoftteams/manage-external-bots
5. https://learn.microsoft.com/microsoftteams/rooms/teams-rooms-people-recognition
6. https://www.priv.gc.ca/en/privacy-topics/surveillance/02_05_d_14?product=crm
7. https://web.mit.edu/parmstr/Public/NRCan/CanBldgDigests/cbd186_e.html
8. https://grc.ca/sites/default/files/doc/gcpsg-gsmgc-017-eng.pdf

9. https://www.nortonrosefulbright.com/en/knowledge/publications/c6639e2c/recording-and-transcribing-meetings-managing-risks-and-maximizing-benefits
10. https://learn.microsoft.com/en-us/microsoftteams/teams-bot-identification
11. https://help.otter.ai/hc/en-us/articles/35973988280215
12. https://docs.granola.ai/help-center/taking-notes/transcription
13. https://learn.microsoft.com/en-us/microsoftteams/who-can-bypass-meeting-lobby
14. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/collecte-renseignements-personnels_entreprises
15. https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1
16. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/renseignement-personnel-definition
17. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/champ-application-loi_entreprises
18. https://www.legisquebec.gouv.qc.ca/fr/document/lc/CCQ-1991
19. https://www.legisquebec.gouv.qc.ca/en/document/cs/CCQ-1991
20. https://laws.justice.gc.ca/eng/acts/c-46/section-183.html
21. https://laws-lois.justice.gc.ca/eng/acts/c-46/section-183.1.html
22. https://langlois.ca/words-fade-away-recordings-remain-admissibility-evidence-audio-video-recordings
23. https://www.priv.gc.ca/en/privacy-topics/privacy-for-businesses/appropriate-handling-of-personal-information/collecting-personal-information-and-consent/consent/gl_omc_201805
24. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda
25. https://educaloi.qc.ca/en/legal-news/digital-surveillance-at-work-can-your-boss-monitor-what-you-do
26. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/utilisation-communication-renseignements-personnels
27. https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf
28. https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127
29. https://help.fathom.video/en/articles/296512
30. https://docs.granola.ai/help-center/consent-security-privacy/security-privacy-data-faqs
31. https://library.zoom.com/ai/ai-whitepaper/data-governance-and-privacy
32. https://learn.microsoft.com/microsoftteams/rooms/voice-recognition
33. https://learn.microsoft.com/microsoftteams/rooms/voice-and-face-recognition
34. https://help.otter.ai/hc/en-us/articles/40643231903639-Disable-Speaker-Learning
35. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/biometrie
36. https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_Biometrie_Organisations.pdf
37. https://store.astm.org/e0413-22.html
38. https://store.astm.org/e1130-16r21.html
39. https://web.mit.edu/parmstr/Public/NRCan/CanBldgDigests/cbd051_e.html
40. https://web.mit.edu/parmstr/Public/NRCan/CanBldgDigests/cbd236_e.html

41. https://learn.microsoft.com/en-gb/microsoftTeams/rooms/room-planning-guidance
42. https://learn.microsoft.com/microsoftteams/hybrid-meetings-device-select
43. https://www.shure.com/en-us/products/microphones/mxa920
44. https://www.jabra.com/en-ca/business/video-conferencing/jabra-panacast-50
45. https://futureisnow.logitech.com/content/dam/logitech/en/video-collaboration/pdf/rally-mic-pod-placement-guide.pdf
46. https://support.microsoft.com/teams/calls-devices/microsoft-teams-rooms-android
47. https://learn.microsoft.com/en-us/microsoftteams/rooms/proximity-join
48. https://support.microsoft.com/en-US/teams/notifications-settings/manage-your-device-settings-in-microsoft-teams
49. https://learn.microsoft.com/microsoftteams/recording-transcription-custom-message
50. https://support.google.com/meet/answer/14754931
51. https://support.google.com/meet/answer/9308681?hl=en
52. https://library.zoom.com/ai/ai-whitepaper/user-transparency-and-notice
53. https://help.otter.ai/hc/en-us/articles/4425393298327-OtterPilot-Overview
54. https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai
55. https://support.microsoft.com/en-us/teams/meetings/start-stop-and-download-live-transcripts-in-microsoft-teams-meetings
56. https://learn.microsoft.com/microsoftteams/tmr-meeting-recording-change
57. https://learn.microsoft.com/en-us/microsoftteams/manage-teams-recording-expiration-policy
58. https://learn.microsoft.com/microsoftteams/meeting-transcription-captions
59. https://learn.microsoft.com/microsoftteams/intelligent-recap-without-saving-transcripts
60. https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057960
61. https://learn.microsoft.com/microsoftteams/copilot-teams-transcription
62. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/conservation-destruction-renseignements-personnels
63. https://help.otter.ai/hc/en-us/articles/360048322533-Speech-transcription-accuracy-FAQ
64. https://guide.fireflies.ai/articles/7003995379-Recording+Consent+and+Meeting+Compliance+in+Fireflies:+Opt-In,+Opt-Out,+and+Controls
65. https://help.fathom.video/en/articles/3239681
66. https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0058013
67. https://www.quebec.ca/nouvelles/actualites/details/loi-25-sur-la-protection-des-renseignements-personnels-des-citoyens-du-quebec-entree-en-vigueur-de-nouvelles-dispositions-qui-font-du-quebec-un-chef-de-file-mondial-50726
68. https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25
69. https://statistique.quebec.ca/en/communique/portrait-teletravail-quebec
70. https://www150.statcan.gc.ca/n1/daily-quotidien/250826/dq250826a-eng.htm
71. https://www.cai.gouv.qc.ca/actualites/ia-au-travail-la-commission-plaide-pour-meilleur-encadrement

THE PUBLISHER

About 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore private offices, day passes and desks, the conference room, business addresses and virtual mailboxes. Book a visit or contact the team to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Website: https://2727coworking.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.