EVERSHEDS SUTHERLAND

Recording with reason

Global employer guide to recording and transcribing internal meetings

For the best possible user experience, download this PDF before viewing

Contents

this is a fully interactive document, click to access content

Global employer guide to recording and transcribing internal meetings

The practice of recording and transcribing internal meetings is increasing across all sectors. An organizer will press the "record (and transcribe)" button at the start and this can help those who do not attend to catch up later, or support with preparing meeting minutes afterwards. AI can often prepare a meeting summary, or a first draft of the minutes. These can be convenient and time-saving actions.

If recording and transcribing meetings in an employment context however, from internal discussions and business planning, to disciplinary, performance management, sickness absence meetings, and more, it is worth pausing before you press "record" to consider potential benefits versus risks.

In this guide, we highlight some of the key data privacy and employment law risks that global employers need to consider and provide top tips to mitigate these, focusing on the following selected jurisdictions and regions:

UK

Europe

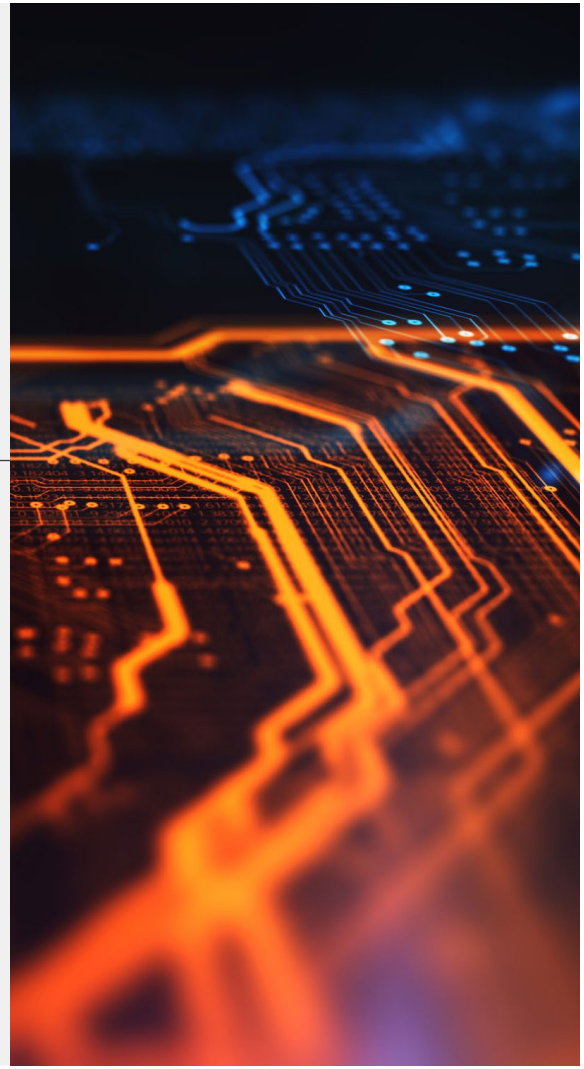
US

Asia
(specifically, Hong Kong, Singapore, and Mainland China)

UK

continue →

1. What are the data privacy implications to consider when recording internal meetings? Do you need to seek the employee's consent if you are recording and/or transcribing the meeting?	Firstly, employers must assess who controls the recording/transcription and the rights of any system providers. Contractual terms are key and should be carefully reviewed when engaging providers. Under UK GDPR, employers must have a lawful basis for processing personal data and an additional lawful basis for processing any special category data (e.g. health information, trade union membership, etc.), together with considering the necessity and proportionality of any such proposed data processing. Special category data triggers stricter rules and higher risks. In some cases, traditional methods, like anonymized handwritten notes may be safer, depending on the meeting's nature.	Employees must be notified of the processing, typically via a privacy notice. Reconfirming at the start of the meeting is best practice to manage expectations and reduce complaints. Under UK GDPR, employers must ensure security and accuracy. AI-generated transcripts can sometimes misrecord content, so human review is essential to meet accuracy obligations. Retention periods should be proportionate, longer storage increases privacy risks. Employers should also prepare for data subject access and erasure requests. If employers retain recordings or transcripts containing personal data, these may need to be disclosed/deleted upon such requests.
2. Are there any specific employment law risks to consider?	When recording or transcribing employment meetings, it is best practice to inform employees at the outset. This will reduce the risk of complaints and later issues. AI-generated transcripts must be checked for accuracy, especially if being relied upon to make employment decisions. Errors linked to accents or speech affected by disability could lead to discrimination claims or undermine procedural fairness and litigation outcomes. A "human in the loop" is essential. Confidentiality is critical. Access to recordings and transcripts should be limited to authorized personnel to avoid data breaches and legal claims.	Employers should implement a clear policy outlining when and how internal meetings may be recorded or transcribed. This promotes transparency and sets expectations for managers and HR teams. Finally, employers should be prepared to consider employee requests for recording or transcription as a reasonable adjustment under the Equality Act 2010 and how this might be responded to, depending on individual circumstances.



UK continued

continue

3. Are there any circumstances where it is unlawful to make a recording or transcription of internal meetings?

From an employment law perspective, there are no explicit bans on recording or transcribing internal meetings; however, there are important employment law considerations to think through first (as above) to avoid complaints and claims.

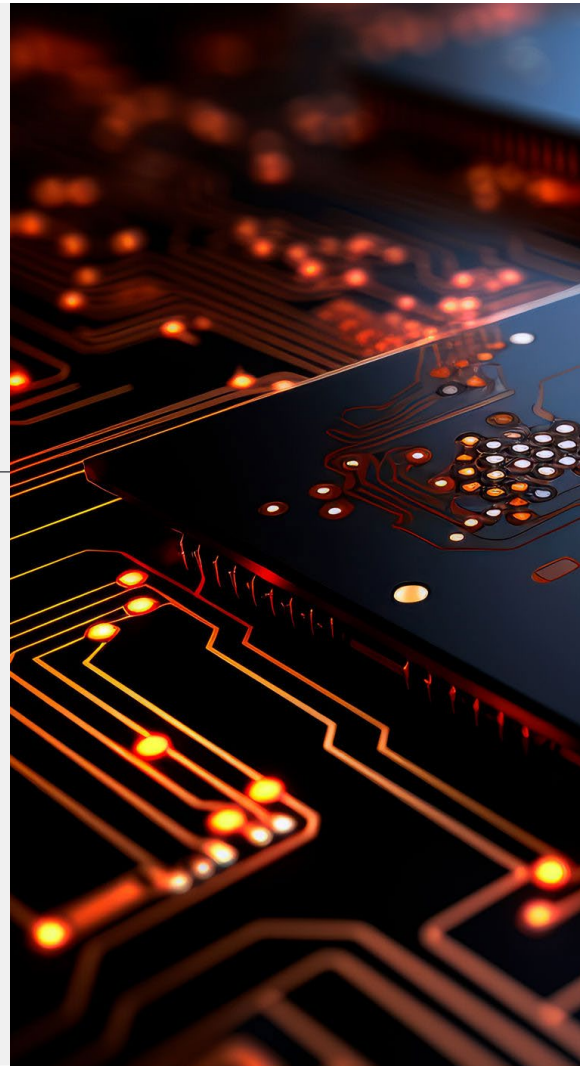
From a data protection perspective, any recording or transcript created without a lawful basis under UK GDPR (or otherwise in breach of data protection laws) would be unlawful. In addition, the following scenarios carry greater risk from a UK data protection compliance perspective:

- where the proposed recordings or transcripts are not covered by the relevant fair processing information (or privacy notice(s)) or where these are not provided to participants, in advance, correctly
- where the meeting is not necessary for business purposes (e.g. social calls with colleagues/contacts)
- where special categories of personal data are likely to be disclosed and the employer does not have a lawful basis for collecting the personal data (for example, where someone is talking about a health, religious, or political matter that it is not necessary to record for the purposes notified to participants)
- where recorded covertly (e.g. where the participants are not notified that the recording is taking place, save for in specific legal situations which are rare)

4. What other risks do I need to be aware of?

If discussing legally privileged matters, employers will also need to take care to protect privilege. For example, if confidentiality is lost (e.g. because the recording is widely accessible), then privilege will also be lost.

Whilst not specifically a legal risk, employers might also want to consider how recording or transcribing a meeting could impact the meeting. For example, would an employee feel comfortable talking freely in a sensitive employment meeting if they were being recorded? This could result in meetings becoming overly formal and failing to achieve their aims.



UK | Top tips

Across all jurisdictions, putting in place these core standards ("**Recommended Global Best Practice**") will support the mitigation of common risks and ensure best practice:

- conduct thorough due diligence and testing of any new third-party AI systems to understand fully how these work, including security settings
- review and align supplier/vendor terms with internal policies and standards when using third-party AI systems
- inform participants before recording/transcribing internal meetings
- include tailored warnings at the start of a recorded/transcribed meeting, around, for example, what should and should not be discussed, e.g. confidentiality and (in applicable jurisdictions and if legal advice is being given) legal privilege
- consider pausing or stopping the recording if sensitive personal/special category data is being discussed
- review AI-generated transcripts for accuracy and ensure there is a "human in the loop" to check output
- implement a clear policy on recording and transcribing internal meetings, setting clear employee standards for use, including the types of meetings that are/are not appropriate for recording and/or transcribing
- consider confidentiality and restrict access to recordings/transcripts to key persons; ensure robust data security
- set proportionate retention periods for recordings and transcripts
- avoid using public AI tools to summarize, transcribe, or record internal meetings as these are not secure and may invite significant legal risks, particularly where personal and sensitive personal/special category data is discussed

In addition to the **Recommended Global Best Practice** (see above), tips for mitigating UK-specific risks include:

- ensure a lawful basis/es under UK GDPR for processing personal and special category data, relying upon employee consent will rarely be compliant in the UK
- ensure data privacy notices are updated accordingly to ensure employees are notified of any data processing, and consider whether a Data Protection Impact Assessment (DPIA) is also required
- bear in mind the Equality Act 2010 and the risk of discrimination claims from protected groups if relying upon inaccurate recordings
- consider the potential for data subject access requests and prepare to respond to these

Europe

continue

1. What are the data privacy implications to consider when recording internal meetings? Do you need to seek the employee's consent if you are recording and/or transcribing the meeting?	The EU GDPR provides the overarching framework, broadly aligned with the UK GDPR, though differences in interpretation and enforcement as a result of local member states implementing legislation. Employers must identify a lawful basis under Article 6 GDPR for recording or transcribing meetings. "Consent" is generally unsuitable in employment due to power imbalances. (It is worth noting, however, that even though consent is rarely suitable for GDPR purposes, some member states require consent for audio recording due to other laws/requirements, and employers should check this.) More typical lawful bases include the employer's "legitimate interests" (balanced against employee rights) or compliance with legal obligations (rarely applicable). If recordings capture special category data (e.g. health or union membership), an additional lawful basis under Article 9 is needed, such as the necessity to comply with obligations in the field of employment law, or where the processing is strictly necessary for the establishment, exercise, or defense of legal claims. Transparency is particularly strict under the GDPR. Employees must be informed in advance via clear, accessible privacy notices that detail the purpose of the recording/transcription, retention periods, who will have access, and third-party provider involvement. Confirming that recording/transcription is taking place at the start of meetings is also best practice. Employers must also clarify whether external providers act as processors (Article 28) or (joint) controllers (Article 26), as this affects contractual and information duties. Accuracy and data minimization are essential. AI-generated transcripts may misrecord information, risking inaccurate data processing in breach of GDPR (and affecting employment decision making). Employers must consider how best to deal with data accuracy challenges to meet the requirements of Article 5. Retention should be proportionate to the stated purpose, with short periods preferred unless justified. Systematic or special category data processing may require that a Data Protection Impact Assessment (DPIA) under Article 35 be undertaken in advance of deployment. Security is critical, especially with external or cloud-based services. Contracts with processors must meet Article 28 requirements, and transfers outside the EEA need appropriate safeguards (e.g. standard contractual clauses). Finally, employees have rights under Chapter III GDPR, including access, rectification, erasure, and objection, which may apply to recordings and transcripts. Employers must be ready to respond to such requests.
2. Are there any specific employment law risks to consider?	If using AI to record or transcribe internal meetings in the EU, employers must determine whether the EU AI Act applies and comply with its requirements where applicable. The AI Act, effective from August 1, 2024, applies to various operators in the AI supply chain including providers, deployers (which will be the majority of employers), and affected persons of AI systems. It covers AI output used in the EU, even if operated from outside the EU, and therefore has an extraterritorial effect. The AI Act adopts a risk-based approach, categorizing AI systems as prohibited, high-risk, limited-risk, or minimal risk. Employers must identify the specific purpose and functionality of any AI-based recording or transcription to determine the applicable risk category and corresponding legal obligations. Prohibited systems include, for example, those that infer emotions in the workplace. High-risk AI systems include (but are not limited to) those intended to be used for recruitment, or to make decisions affecting terms of work-related relationships. Before implementing any high-risk AI system, employers (as deployers) must, amongst other measures, inform workers' representatives and affected employees, in accordance with Union and national law and practice. Most requirements relating to high-risk AI systems will take effect from August 2, 2026. Employee representative involvement in new workplace technology is already required in many EU Member States, especially where technology monitors behavior or performance. The AI Act now establishes a baseline requirement across the EU for such involvement in relation to AI systems. The AI Act also introduces AI literacy requirements, effective from February 2, 2025. Organizations developing or using AI systems must ensure staff and other relevant individuals are sufficiently AI literate, with appropriate measures tailored to the specific context of AI use. The obligations to inform employee representatives and to ensure AI literacy are connected and often overlap and may be reinforced by national regulations requiring consultation or agreement before introducing new workplace technology. Adequate information must be provided about the functionality and potential impact of the AI system, typically through training and information sessions. In addition to compliance with the AI Act, employers must ensure that AI-generated transcripts are checked for accuracy, particularly if relied upon for employment decisions. Errors related to accents or speech affected by disability could result in discrimination claims or undermine procedural fairness and litigation outcomes. Human oversight ("human in the loop") is essential and also a requirement under the EU AI Act for high-risk systems. Confidentiality remains critical: access to recordings and transcripts should be limited to authorized personnel to prevent data breaches and legal claims. Employers should implement a clear policy outlining when and how internal meetings may be recorded or transcribed, promoting transparency and setting expectations for managers and HR teams.

Europe continued

continue →

3. Are there any circumstances where it is unlawful to make a recording or transcription of internal meetings?

Recording or transcribing internal meetings is not generally prohibited under EU employment law, but it may become unlawful if it breaches data protection rules, labor law principles, or civil codes protecting personality rights.

Under GDPR, recordings without a valid lawful basis are unlawful. Key risks include:

- **Transparency failures:** Employees must be informed in advance via privacy notices or at the meeting's start. Covert recording is illegal in many Member States, e.g. a criminal offence in Germany (§201 StGB), and incompatible with labor/privacy rules in France. In the Netherlands, one-party recording is not criminal but may still breach employment or civil law.
- **Lack of necessity/proportionality:** Recordings must serve a legitimate business need. Capturing informal or unjustified meetings likely breaches Article 5(1)(c) GDPR.
- **Special category data:** If sensitive data (e.g. health, religion, union membership) may be discussed, an Article 9 basis is required. Without it, processing is unlawful.
- **Employment law and works council rights:** as above, employers must ensure compliance with potential information and consultation obligations when introducing new AI systems, whether under the EU AI Act or national laws.
- **Civil law restrictions:** Many Member States protect employee dignity and privacy under civil or constitutional law. Recording without clear justification or consent may infringe these rights, even if GDPR is formally followed, and could lead to damages claims.

In practice, recordings are only lawful if they are transparent, justified, limited in scope, and supported by valid legal bases under both data protection and employment law. Regulators and courts often apply stricter standards where workplace power imbalances exist.

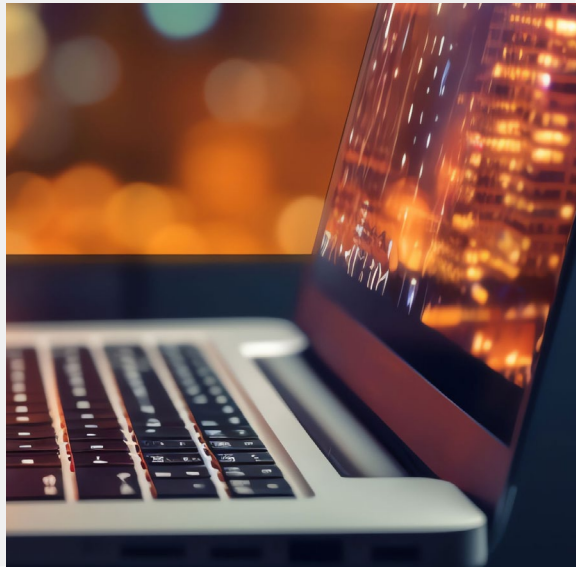
4. What other risks do I need to be aware of?

In the EU, recording legally privileged discussions requires caution. If recordings or transcripts are not securely stored or access is poorly controlled, confidentiality, and in some jurisdictions, legal privilege, may be lost, especially in litigation. Privilege rules vary; communications with external EEA-admitted lawyers are generally protected, but in-house counsel may not be. Employers should exclude legal strategy discussions from recordings or apply enhanced safeguards.

From an employment relations perspective, recording can affect workplace culture. Trust, good faith, and dignity are central in many EU jurisdictions. Employees may feel inhibited in sensitive meetings (e.g. disciplinary or health-related) if they know they are being recorded, potentially undermining the process and raising fairness concerns in disputes.

Works councils and trade unions may also object to the "chilling effect" of recording technologies. Failing to engage with these concerns can lead to industrial relations issues beyond legal compliance.

Reputational risk is another factor. Accidental disclosure, via data breach or subject access request could expose sensitive internal discussions. EU regulators increasingly assess not just GDPR compliance, but whether employers act fairly and proportionately in practice.



Europe | Top tips

In addition to the **Recommended Global Best Practice** (see above), tips for mitigating EU-specific risks include:

- map out the AI systems being used, including the purpose of such use, the functionality, and any risks associated with such use, to identify any prohibited AI systems and to identify any high-risk systems under the AI Act
- bear in mind the extra-territorial reach of the AI Act
- assess the current level of AI literacy within the organization and implement measures to comply with AI literacy requirements
- do not overlook obligations to inform employee representatives, both in compliance with requirements under the AI Act and any additional national law and practice requirements on the introduction of new or updated AI systems (regardless of any legal obligations to do so, keeping the workforce informed about the use of AI can support good employee relations and foster workforce trust and confidence in AI)
- ensure a lawful basis/es under GDPR for processing personal and sensitive personal data, relying upon consent will rarely be compliant in the EU
- update data privacy notices
- document necessity and proportionality, under the GDPR, employers should be able to demonstrate why recording was the least intrusive option for the stated purpose, and a short internal DPIA (data protection impact assessment) can help evidence this
- check international data transfers, and if recordings or transcripts are processed outside the EEA (for example, by cloud-based AI providers), ensure that valid transfer safeguards are in place, such as Standard Contractual Clauses or adequacy decisions
- ensure exercise of data subject rights, employers should be aware of the effects of these rights and have a process in place to comply with such requests

US

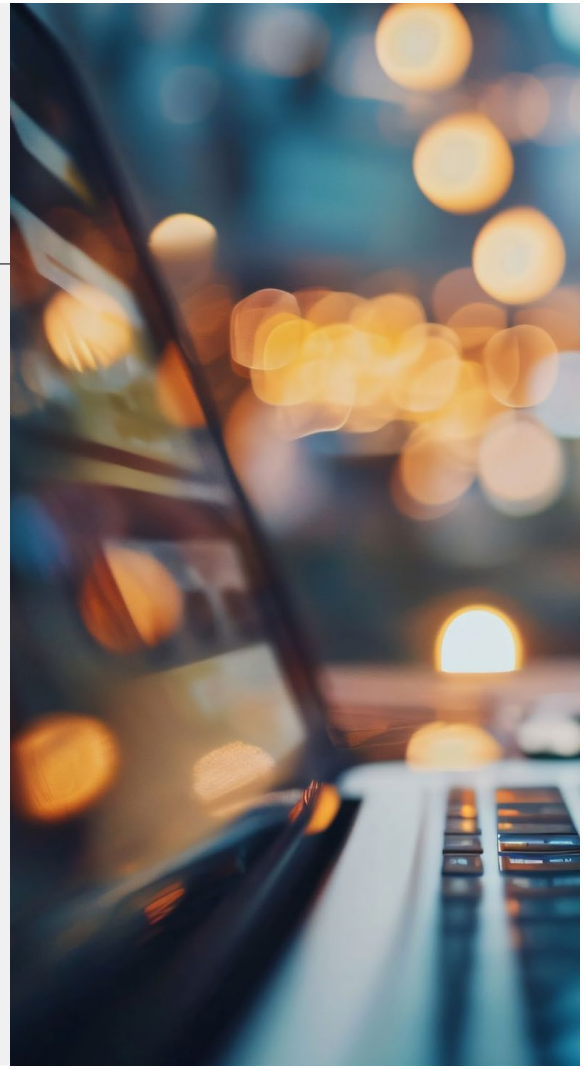
continue →

1. What are the data privacy implications to consider when recording internal meetings? Do you need to seek the employee's consent if you are recording and/or transcribing the meeting?	In general, there is no prohibition on recording and transcribing meetings that are held on employer-owned property or through employer-managed channels (e.g. a virtual call that the employer organized). If the recording includes audio, an employer may need to obtain the employee's consent before recording, as some states are two-party consent states (i.e., both the party recording and the party being recorded must consent). While states guidelines on consent vary, the general theme is that the notice and consent must be meaningful. Given the administrative challenge of sifting through state laws, providing the employee with notice and obtaining their consent prior to recording is generally recommended to mitigate risk. If the meeting being recorded involves participants from multiple states, employers should default to the most restrictive law.	Employers must also consider the nature of the information being recorded. If the recording captures personal information, it is important to heed the widespread state legislation requiring reasonable safeguards, security controls, and a breach notification when collecting and storing data about that state's residents. Further, if the AI tool has access to other interlinked systems (for example, it pulls a file as a reference if it is mentioned on the call), it is important to consider any access controls that may be necessitated by data protection laws. For example, if sensitive data, medical data, or protected health information (PHI) is involved, this may trigger additional obligations under laws such as the Americans with Disabilities Act (ADA) and Health Insurance Portability and Accountability Act 1996 (HIPAA).	Employers should also vet third-party vendors for compliance and ensure that their data protection practices are aligned with their own, since, if vendors are seen as acting as the employer's agent, their negligence is likely to be attributed to the employer in the event of a claim. Retention policies should be clear, and employers should be prepared to respond to access or deletion requests in states where such rights exist (e.g. California)
2. Are there any specific employment law risks to consider?	As above, providing notice and seeking consent is recommended. It will be important to review any AI-generated transcriptions to ensure accuracy and maintain a "human in the loop", particularly if the transcript is relied upon as the basis for an employment decision. If an AI transcription were inaccurate because of an employee's accent or a disability impacting speech, this could result in potential employment claims, including discrimination. Further, if the transcription-based decision results in disparate impact on a particular category, that could also be the basis for a discrimination claim. Without any human oversight, such claims can be challenging to defend as facts become harder to recall over time.	In addition, if there are no access controls in place, and transcription results in unintended sharing of confidential data, this could lead to potential violations of laws such as the ADA. Also, if a hiring manager becomes aware of a protected trait, such as a disability, through the transcription process and then makes an adverse employment decision, even if it is unrelated to the disability, an employer could be left incurring substantial legal fees to defend its decision. A significant risk of using transcription is that the AI-generated transcription, which may memorialize strategic decision-making processes, could be discoverable and used against the employer in a proceeding.	Also, if sensitive conversations, such as a union discussion or activity protected under the National Labor Relations Act, are recorded and acts to deter the activity, the recording/transcription could be seen as a violation of the NLRA. Therefore, it is important to ensure that such conversations are not recorded by the employer. It is also important to consider any union-related concerns and the terms of collective bargaining agreements before deploying any employee technology.

US continued

continue →

3. Are there any circumstances where it is unlawful to make a recording or transcription of internal meetings?	There are no explicit bans on recording or transcribing internal meetings; however, there are important employment and data privacy considerations to think through first (as above) to avoid complaints and claims.
4. What other risks do I need to be aware of?	As discussed above, if discussing legally privileged matters, employers will also need to take care to protect privilege. AI-generated transcripts risk being treated as discoverable documents if the vendor is not bound by guarantees and confidentiality protections, and this is further exacerbated by the lack of reliability in the absence of human oversight. Using AI technology to transcribe meetings may also create additional discoverable items, as any metadata or analytical outputs produced based on an otherwise discoverable transcript may also be considered discoverable. Whilst not specifically a legal risk, employers might also want to consider how recording or transcribing a meeting could impact the meeting. For example, would an employee feel comfortable talking freely in a sensitive employment meeting if they were being recorded? This could result in meetings becoming overly formal and not achieving its aims. Further, a lack of controls around the dissemination of a meeting transcription could lead to the leak of trade secrets and confidential information. This is particularly the case in the case of AI tools, if say vendors are not restricted by contract from using confidential data to train the AI model.



US | Top tips

In addition to the **Recommended Global Best Practice** (see above), tips for mitigating US-specific risks include:

- ensure that vendor contracts contain confidentiality protections and guarantees (such as ensuring the data will not be used to train any AI models) and set forth liability parameters
- provide meaningful notice and opportunity to consent, notice should be understandable and straightforward, and consent should be clear
- be prepared to respond to access or deletion requests under state laws (e.g., under California law)
- consider union/collective bargaining agreement requirements before deploying new technology
- protect legally privileged matters, AI transcripts may be discoverable in litigation
- think twice before recording sensitive conversations that could be discoverable or lead to the allegation of an illegal employment action such as discrimination or retaliation

Asia

continue →

	Hong Kong	Singapore	Mainland China **(excluding for the purposes of this guide Hong Kong SAR, Macau SAR and Taiwan)**
1. What are the data privacy implications to consider when recording internal meetings? Do you need to seek the employee's consent if you are recording and/or transcribing the meeting?	Employees must be notified if a meeting is recorded, especially if they can be identified or if the recording will be used to compile information about them. This is required under the Data Protection Principles (DPPs) of the Personal Data (Privacy) Ordinance (PDPO). While prior consent is not always necessary, failing to inform employees may be unlawful. Recordings should be securely stored and there should be a timetable for their destruction.	Employers should obtain written consent from employees before recording internal meetings. This is typically obtained through employment contracts or employee handbooks. While the Personal Data Protection Act 2012 (PDPA) provides for some exemptions from consent, it is recommended that employers still seek express consent. Recordings must be securely stored and there should be a timetable for their destruction.	Explicit consent from employees is generally required for recording internal meetings, in line with the Personal Information Protection Law (PIPL). This separate consent must be specific, unbundled, and clearly authorized, checkbox consent to a general privacy policy is not sufficient. Unlike jurisdictions such as the UK/EU, the PIPL does not recognize "legitimate interests" as a basis for processing personal data, so organizations must rely on explicit consent or HR management necessity. Separate consent is needed for processing sensitive data and cross-border transfers. Recordings stored outside Mainland China must comply with PIPL requirements, including conducting a Personal Information Protection Impact Assessment (PIPIA) and, if necessary, signing Chinese Standard Contractual Clauses (SCCs).
2. Are there any specific employment law risks to consider?	As above, inform employees and obtain express consent before recording or transcribing meetings. Ensure AI transcription accuracy to avoid discrimination claims. Maintain clear internal policies on recording and transcribing meetings, including security measures and retention periods. Erase personal data when no longer needed, unless legally required to retain it.	Inform employees and obtain express consent before recording or transcribing meetings to avoid complaints. Check AI transcriptions for accuracy and be mindful of the newly passed Workplace Fairness Act 2025 (not yet in effect and expected to be implemented sometime in 2026 or 2027), which prohibits discrimination based on protected characteristics. Ensure AI tools do not create unfair advantages or disadvantages due to different language backgrounds. Implement clear policies for recording and securely storing meeting records.	Employment law risks are unlikely to arise. Under PRC law, from an evidence perspective, as long as the recording does not infringe on others' right to privacy (e.g. the recording is made in relatively public settings such as offices or meeting rooms in workplace), it is generally considered legal and valid even if the other party is unaware of it. Therefore, when recording and/or transcribing an employment meeting, it is not necessary to inform the employee at the outset of each meeting or to ask for their consent from an employment law perspective.

Asia continued

continue →

	Hong Kong	Singapore	Mainland China (excluding for the purposes of this guide Hong Kong SAR, Macau SAR and Taiwan)
3. Are there any circumstances where it is unlawful to make a recording or transcription of internal meetings?	From an employment law perspective, there are no explicit bans on recording or transcribing internal meetings; however, important employment law considerations must be addressed to avoid complaints and claims. From a data privacy perspective, provided the employee is adequately notified of the recording, there is no explicit ban on recording or transcribing internal meetings.	From an employment law perspective, there are no explicit bans on recording or transcribing internal meetings; however, important employment law considerations must be addressed to avoid complaints and claims. From a data privacy perspective, any recording or transcript created without consent or notification of the purpose would be unlawful if no statutory exemptions apply. Using a recording or transcript beyond the stated purpose may violate the purpose limitation obligation under the PDPA.	N/A, see comments above.
4. What other risks do I need to be aware of?	Employers must protect legally privileged matters during recordings. Risks include unintended leakage of personal data. Employees have the right to access and correct their data, but employers can refuse access under specific conditions, such as crime prevention or disciplinary processes.	Employers must protect legally privileged matters during recordings. Data breaches are a risk under the PDPA, requiring notification to affected employees and the PDPC within three days if significant harm is likely. Sensitive data includes pay, health status, sexual offence allegations, and mental health assessments. Employees have the right to access and correct their data, but employers can refuse access under specific conditions.	Recordings used as evidence in disputes require the original medium for authenticity verification. Employers should safeguard the original recording equipment.

Asia | Top tips

In addition to the **Recommended Global Best Practice** (see above), tips for mitigating Asia-specific risks include:

- in Singapore and China, obtain express notified consent before recording
- be prepared to respond to data subject requests
- check international data transfers (especially for Mainland China), and if recordings or transcripts are processed or stored outside Mainland China, ensure that valid transfer safeguards are in place

Final reflections

For employers who are considering the issue of recording and/or transcribing internal meetings using AI across their global workforce, there are a myriad of global laws to understand and comply with. While there are some common themes across jurisdictions, including the need for transparency, robust data privacy and security measures, clear internal policies, and human oversight of AI-generated outputs, there are also crucial differences. These include variations in consent requirements, the scope of employee rights, the definition and treatment of sensitive data, and the approach to AI risk categorization and regulatory enforcement.

Given the complexity and evolving nature of the legal landscape, employers should always seek specialist legal advice to ensure compliance with all applicable laws and best practice.

Our global team of specialist AI lawyers at Eversheds Sutherland is at the forefront of advising on the intersection of technology and employment and data privacy law. We regularly support clients with:

- navigating global AI and employment law developments, including the EU AI Act
- building AI compliance frameworks and policies for HR and legal teams
- understanding global data privacy requirements
- completing global and local audits of workforce-related risks
- delivering practical training for HR and in-house counsel on AI, to support both innovation and compliance

For further information, or to discuss how we can support your organization, please contact your usual Eversheds Sutherland contact, or those individuals detailed in this guide.

Getting in touch

UK

Hannah Wilkins
Partner
T: +44 121 232 1558
M: +44 779 564 6288
hannahwilkins@
eversheds-sutherland.com

Hannah Mahon
Partner
T: +44 207 919 0676
M: +44 755 380 0248
hannahmahon@
eversheds-sutherland.com

Dave Hughes
Partner
T: +44 122 344 3642
M: +44 782 793 6225
davidlhughes@
eversheds-sutherland.com

Europe

Stefan Corbanie
Partner, Belgium
T: +32 2 737 9351
M: +32 486 453 149
stefancorbanie@
eversheds-sutherland.com

Deborah Attali
Head of Employment Law Team, France
T: +33 1 55 73 42 17
M: +33 6 47 58 88 95
deborahattali@
eversheds-sutherland.com

Frank Achilles
Partner, Germany
T: +49 89 5456 5275
M: +49 151 5711 7481
frankachilles@
eversheds-sutherland.com

Marieke Koster
Partner, Netherlands
T: +31 10 248 8057
M: +31 627 359 547
mariekekoster@
eversheds-sutherland.com

Robbert Santifort
Principal Associate, Netherlands
T: +31 10 248 8077
robbertsantifort@
eversheds-sutherland.com

Ilham Ezzamouri
Associate, Netherlands
T: +31 10 248 8063
ilhamezzamouri@
eversheds-sutherland.com

US

Deepa Menon
Partner, Washington DC
T: +1 202 383 0928
deepamenon@
eversheds-sutherland.com

Michael Hepburn
Partner, Washington DC
T: +1 202 383 0104
michaelhepburn@
eversheds-sutherland.com

Asia

Jack Cai
Managing Partner, Mainland China
T: +86 21 6137 1007
M: +86 189 3080 1987
jackcai@
eversheds-sutherland.com

Frankie Tam
Partner, Hong Kong
T: +852 2186 4919
M: +852 9252 5819
frankietam@
eversheds-sutherland.com

EVERSHEDS
SUTHERLAND

eversheds-sutherland.com

DTUK005558_V4